

# Symantec Decoy Server 3.1 Implementation Guide

# Symantec Decoy Server 3.1

## Implementation Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version 3.1

PN: 10059354

### Copyright Notice

Copyright © 2003 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

NO WARRANTY. The technical documentation is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

### Trademarks

Symantec and the Symantec logo are U.S. registered trademarks of Symantec Corporation. Windows is a registered trademark, and 95, 98, NT and 2002 are trademarks of Microsoft Corporation. Sun is a registered trademark, and Java, Solaris, Ultra, Enterprise, and SPARC are trademarks of Sun Microsystems. UNIX is a registered trademark of UNIX System Laboratories, Inc. Pentium is a registered trademark of Intel Corporation. iButton is a trademark of Dallas Semiconductor Corp.

Symantec Decoy Server software includes the following Third Party Software from external sources: “bzip2” and associated library “libbzip2,” Copyright © 1996-1998, Julian R Seward. All rights reserved. Portions of the Symantec Decoy Server software were contributed from external sources. The individuals and their copyrights are listed below:

Copyright © 2002 Matthias L. Jugel and Marcus Meißner

Copyright © 1996-2000 Julian R. Seward. All rights reserved.

Copyright © 1989, 1991, 1992 by Carnegie Mellon University (derivative work)

Copyright © 1995-1998 Jean-loup Gailly and Mark Adler

Copyright © 1995 Tatu Ylonen, Finland

Symantec Decoy Server includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>). Copyright (c) 1998-2000 The OpenSSL Project.

Symantec Decoy Server includes cryptographic software written by Eric Young (eay@cryptsoft.com) and Tim Hudson (tjh@cryptsoft.com). All rights reserved.

Symantec Decoy Server Software contains software developed by the University of California, Berkeley and its contributors. Copyright 1994, 1995, 1996, 1997, 1998. The Regents of the University of California. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Copyright © 1996, 1998, 1999, 2000. The Regents of the University of California. All rights reserved.

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

# Technical support

As part of Symantec Security Response, the Symantec global Technical Support group maintains support centers throughout the world. The Technical Support group's primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our Web-accessible Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering as well as Symantec Security Response to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Symantec technical support offerings include:

- n A range of support options that give you the flexibility to select the right amount of service for any size organization
- n Telephone and Web support components that provide rapid response and up-to-the-minute information
- n Upgrade insurance that delivers automatic software upgrade protection
- n Content Updates for virus definitions and security signatures that ensure the highest level of protection
- n Global support from Symantec Security Response experts, which is available 24 hours a day, 7 days a week worldwide in a variety of languages
- n Advanced features, such as the Symantec Alerting Service and Technical Account Manager role, offer enhanced response and proactive security support

Please visit our technical support Web site at <http://www.symantec.com/techsupp/> for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product that you are using.

## Licensing and registration

If the product that you are implementing requires registration and/or a license key, the fastest and easiest way to register your service is to access the Symantec licensing and registration site at [www.symantec.com/certificate](http://www.symantec.com/certificate). Alternatively, you may go to [www.symantec.com/techsupp/ent/enterprise.html](http://www.symantec.com/techsupp/ent/enterprise.html), select the product that you wish to register, and from the Product Home Page, select the Licensing and Registration link.

## Contacting Technical Support

Customers with a current support agreement may contact the Technical Support group via phone or online at [www.symantec.com/techsupp](http://www.symantec.com/techsupp).

Customers with Platinum support agreements may contact Platinum Technical Support via the Platinum Web site at [www-secure.symantec.com/platinum/](http://www-secure.symantec.com/platinum/).

When contacting the Technical Support group, please have the following:

- n Product release level
- n Hardware information
- n Available memory, disk space, NIC information
- n Operating system
- n Version and patch level
- n Network topology
- n Router, gateway, and IP address information
- n Problem description
  - n Error messages/log files
  - n Troubleshooting performed prior to contacting Symantec
  - n Recent software configuration changes and/or network changes

## Customer Service

To contact Enterprise Customer Service online, go to [www.symantec.com](http://www.symantec.com), select the appropriate Global Site for your country, then choose Service and Support. Customer Service is available to assist with the following types of issues:

- n Questions regarding product licensing or serialization
- n Product registration updates such as address or name changes
- n General product information (features, language availability, local dealers)
- n Latest information on product updates and upgrades
- n Information on upgrade insurance and maintenance contracts
- n Information on Symantec Value License Program
- n Advice on Symantec's technical support options
- n Nontechnical presales questions
- n Missing or defective CD-ROMs or manuals

# SYMANTEC SOFTWARE LICENSE AGREEMENT

## SYMANTEC DECOY SERVER

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY BEFORE USING THE SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND THE LICENSOR. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR LOADING THE SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE", "NO" BUTTON, OR OTHERWISE INDICATE REFUSAL AND MAKE NO FURTHER USE OF THE SOFTWARE.

### 1. License.

The software and documentation and iButton and documentation that accompanies this license (collectively the "Software") is the proprietary property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, You will have certain rights to use the Software after Your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to You. Except as may be modified by an applicable Symantec license certificate, license coupon, or license key (each a "License Module") that accompanies, precedes, or follows this license, Your rights and obligations with respect to the use of this Software are as follows:

You may:

- A. use that number of copies of the Software and iButton(s), as have been licensed to You by Symantec under a License Module for Your internal business purposes. Your License Module shall constitute proof of Your right to make such copies. If no License Module accompanies, precedes, or follows this license, You may make one copy of the Software you are authorized to use on a single machine.
- B. make one copy of the Software for archival purposes, or copy the Software onto the hard disk of Your computer and retain the original for archival purposes;
- C. use each licensed copy of the Software on a single machine;
- E. only configure the number of cages (virtual environments designed to represent a server machine) as set forth in the License Module;
- E. after written consent from Symantec, transfer the Software on a permanent basis to another person or entity, provided that You retain no copies of the Software and the transferee agrees to the terms of this license; and
- F. use the Software in accordance with any additional permitted uses set forth in Section 9, below.

You may not:

- A. copy the printed documentation which accompanies the Software;
- B. configure more than the number of cages set forth in the License Module
- C. sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt

to discover the source code of the Software, or create derivative works from the Software;

C. use a previous version or copy of the Software after You have received a disk replacement set or an upgraded version. Upon upgrading the Software, all copies of the prior version must be destroyed;

D. use a later version of the Software than is provided herewith unless You have purchased corresponding maintenance and/or upgrade insurance or have otherwise separately acquired the right to use such later version;

E. use, if You received the software distributed on media containing multiple Symantec products, any Symantec software on the media for which You have not received a permission in a License Module;

F. use the Software in any manner not authorized by this license ; nor

G. use the Software in any manner that contradicts any additional restrictions set forth in Section 9, below.

### 2. Content Updates:

Certain Software utilize content which is updated from time to time (including but not limited to the following Software: antivirus software utilize updated virus definitions; content filtering software utilize updated URL lists; some firewall software utilize updated firewall rules; and vulnerability assessment products utilize updated vulnerability data; these updates are collectively referred to as "Content Updates"). You shall have the right to obtain Content Updates for any period for which You have purchased maintenance, except for those Content Updates which Symantec elects to make available by separate paid subscription, or for any period for which You have otherwise separately acquired the right to obtain Content Updates. Symantec reserves the right to designate specified Content Updates as requiring purchase of a separate subscription at any time and without notice to You; provided, however, that if You purchase maintenance hereunder that includes particular Content Updates on the date of purchase, You will not have to pay an additional fee to continue receiving such Content Updates through the term of such maintenance even if Symantec designates such Content Updates as requiring separate purchase. This License does not otherwise permit Licensee to obtain and use Content Updates.

### 3. Product Installation and Required Activation:

This Software contains enforcement technology that limits the ability to install and uninstall the Software on a machine more than a finite number of times for a finite number of machines. This License and the Software containing enforcement technology require activation as further set forth in the Documentation. The Software will only operate for a finite period of time prior to Software activation by You. During activation You will provide Your unique activation key accompanying the Software and PC configuration in the form of an alphanumeric code over the Internet to verify the authenticity of the Software. If You do not complete the activation within the finite period of time set forth in the Documentation or as prompted by the Software, the Software will cease to function until activation is complete, which will restore Software functionality. In the event You are not able to activate the Software, You may contact Symantec Customer Support at the URL and telephone number set forth in the Documentation.

### 4. Limited Warranty:

Symantec warrants that the media on which the Software is distributed will be free from defects for a period of sixty (60) days from the date of delivery of the Software to you. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to Symantec within the warranty period or refund the money you paid for the Software. Symantec does not

warrant that the Software will meet your requirements or that operation of the Software will be uninterrupted or that the Software will be error-free.

If applicable, Symantec warrants that the iButton shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the iButton for a period of 180 days from the date of purchase. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective iButton returned to Symantec within the warranty period or refund the applicable portion of the fees You paid for the iButton.

THE ABOVE WARRANTY IS EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE AND COUNTRY TO COUNTRY.

#### 5. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S LIABILITY EXCEED THE PURCHASE PRICE FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

#### 6. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014, United States of America.

#### 7. Export Regulation:

Export, re-export of this Software is governed by the laws and regulations of the United States and import laws and regulations of certain other countries. Export or re-export of Software to any entity on the Denied Parties List and other lists promulgated by various agencies of the United States Federal Government is strictly prohibited.

#### 8. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Software and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software. The disclaimers of warranties and damages and limitations on liability shall survive termination. Software and documentation is delivered Ex Works California, U.S.A. or Dublin, Ireland respectively (ICC INCOTERMS 2000). This Agreement may only be modified by a License Module which accompanies this license or by a written document which has been signed by both You and Symantec. Should You have any questions concerning this Agreement, or if You desire to contact Symantec for any reason, please write to: (i) Symantec Customer Service, 555 International Way, Springfield, OR 97477, U.S.A., (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland, or (iii) Symantec Customer Service, 1 Julius Ave, North Ryde, NSW 2113, Australia.

#### 9. Additional Uses and Restrictions:

A. You may not create additional classes, interfaces, or subpackages that are contained in the "java" or "sun" packages or similar as specified by Sun Microsystems in any class file naming convention.

B. You may only use the number of iButton devices as set forth in the applicable License Module. Otherwise, You have no rights to use the iButton device. You must separately purchase applicable maintenance and support for the iButton device.



# Contents

Chapter 1	Introducing Symantec™ Decoy Server	
	About Symantec Decoy Server .....	2
	Symantec Decoy Server in action .....	2
	Prevention, detection and response .....	2
	Content Generation Module (CGM) .....	4
	Administration console .....	4
	iButton .....	5
Chapter 2	Deploying Symantec Decoy Server	
	About deploying Symantec Decoy Server .....	8
	Getting started .....	8
	Deployment schemes .....	8
	Minefield deployment scheme .....	9
	Honey Net deployment scheme .....	10
	Shield deployment scheme .....	11
	Custom deployment .....	11
Chapter 3	Installing the Host Software	
	About installing the host software .....	14
	Getting started .....	14
	System requirements .....	15
	Pre-installation .....	16
	Installing Solaris .....	17
	Verifying the Solaris installation .....	18
	Installing network interface cards .....	18
	Using MAC addresses .....	19
	Installing Symantec Decoy Server .....	19
	Choosing a token .....	20
	Installing a hardware token .....	20
	Installing a software token .....	21
	Loading the installation media .....	22
	Configuring Symantec Decoy Server .....	22
	Creating a host configuration .....	23
	Creating a cage configuration .....	25
	Installing host and cage configuration values .....	30

Loading an existing configuration .....	31
Auto-installation .....	31
Remote installation .....	32
Uninstalling Symantec Decoy Server .....	33
Starting and stopping Symantec Decoy Server .....	33
Upgrading Symantec Decoy Server .....	34
Symantec Decoy Server processes .....	35

## Chapter 4     Installing the Administration Console

About installing the administration console .....	38
Installing the administration console .....	38
System requirements .....	38
Installing the administration console on Windows .....	39
Installing the administration console on Solaris .....	40
Uninstalling the administration console .....	41
Starting and stopping the administration console .....	41
Adding local accounts .....	42
Changing the passphrase .....	42
Adding host connections .....	42
Connecting to hosts .....	44
Viewing cages .....	45
Disconnecting from hosts .....	47
Deleting host connections .....	47
Changing host passphrases .....	47
Connecting to the host using SSH .....	48
Adding user accounts .....	50
User account privileges .....	51
Uninstalling the Administration Console .....	52

## Chapter 5     Activating product licenses

About the Symantec Enterprise Licensing System .....	54
License warning and grace periods .....	54
Activating a license .....	54
Activating a license for upgrades .....	55
Removing a License .....	56

## Chapter 6     Setting Parameters

About setting parameters .....	58
Editing parameters from the administration console .....	58
Editing host parameters .....	58
Editing cage parameters .....	60
Saving parameter changes .....	62

Restarting hosts and cages .....	62
Reverting host and cage parameters .....	62
Editing parameters from the command line .....	62
Command line parameters .....	63

## Chapter 7      Configuring Response Policies

About configuring response policies .....	66
Configuring response policies .....	66
Adding response policies .....	66
Selecting events .....	68
Modifying response policies .....	68
Understanding response filters .....	69
Response filter format .....	69
Response filter options .....	70
Adding response filters .....	71
Selecting response filters .....	71
Initiating a response .....	72

## Chapter 8      Creating Reports

About creating reports .....	76
Selecting report types and parameters .....	76
General report options .....	76
Scheduling options .....	81
Date range options .....	82
Data filter options .....	82
Data display options .....	85
Custom query editing options .....	86
Generating reports .....	86
Displaying report options .....	87
Generating reports though the log viewer .....	87

## Chapter 9      Managing Cage Sessions

About managing cage sessions .....	90
Getting started .....	90
Adding a cage user account .....	90
Setting the user password .....	90
Setting the cage root password .....	91
Running cage sessions .....	91
Establishing a cage session .....	92
Editing cage IP addresses .....	92
Editing CGM user accounts .....	92
Modifying cages bypassing the log .....	95

Starting and stopping cages .....	95
Backing up cages .....	96
Restoring cages .....	97
Creating a custom cage .....	97
Web server .....	98
FTP server .....	99
Database server .....	99
Creating a legal disclaimer banner .....	100
Example of a legal disclaimer banner .....	100

## Chapter 10 Managing the Log Database

About managing the log database .....	102
Creating queries .....	102
Adding predefined queries .....	102
Adding custom queries .....	103
Querying log records .....	107
Search limit .....	108
Query search parameters .....	109
Replaying sessions .....	112
Verifying log records .....	113
Log verification failure .....	114
Rotating and compressing log records .....	115
Verifying total log records .....	115
Trimming log records .....	116
Manually compressing log records .....	117
Automatically compressing log records .....	117
Restoring logs .....	118
Restoring backup logs .....	118
Restoring compressed logs .....	119

## Chapter 11 Responding to Attacks

About responding to attacks .....	122
Determining IP ownership .....	122
Taking legal action .....	123

## Chapter 12 Troubleshooting

Configuration checker .....	126
Installation errors and solutions .....	126
Host verification .....	126
Cannot access floppy drive .....	127
System crash during restart .....	127

Wrong OS .....	127
Lack of permissions .....	127
Problem accessing the certificate .....	127
iButton installation problems .....	128
Lack of disk space .....	128
Insufficient resources .....	128
Administration console errors and solutions .....	129
Login screen hangs .....	129
SSH failed connection .....	129
Missing Java or wrong Java version .....	129
Time out .....	130
Alerting errors and solutions .....	131
Wrong SMTP gateway .....	131
Wrong email address .....	131
Wrong mail server .....	132
iButton errors and solutions .....	132
iButton expired .....	132
Wrong communication port .....	132
Cable not securely attached .....	133
iButton not securely seated .....	133
Testing an iButton .....	133
Replacing a faulty or expired iButton .....	133
Cage failure .....	134
Reporting problems .....	134

## Appendix A Event Types

About event types .....	136
Host events .....	136
Administrative (rti.admind) events .....	137
Stealth (rti.stealthd) events .....	138
All module events .....	142
Kernel (rti.klogd) events .....	143
Proc (rti.procs) events .....	144
Sysblock (rti.sysblock) events .....	145
Filesystem (rti.filesys) events .....	146
Cage events .....	147
File (rti.strlog) events .....	147
Process (rti.proclog) events .....	149
File (rti.filelog) events .....	151
Sniffer (rti.sniffd) events .....	152

## Index



# Introducing Symantec™ Decoy Server

This chapter includes the following topics:

- [About Symantec Decoy Server](#)
- [Symantec Decoy Server in action](#)

## About Symantec Decoy Server

Symantec Decoy Server is a deception-based Intrusion Detection System (DIDS) that provides an added layer of defense to your existing network security policy by becoming the target environment of the attack. These controlled deception environments, called cages, log threats in real-time to give your enterprise crucial information about the attack.

## Symantec Decoy Server in action

When an intruder attacks and gains access to a cage, it appears to him as a separate physical system. He is unaware that the master operating system is monitoring every keystroke. SDS provides up to four virtual cages, each running a fully functional copy of the Solaris™ operating system, as it exists on the host machine, and places it into a new directory within that file system. The cages are controlled environments from which the attacker is unable to exit and attack the host system. The effect is four decoy servers with one physical system.

Although the configuration options are endless, a sample configuration would have each cage mimic an organization's FTP, HTTP, SMTP, or SQL servers. This capability greatly reduces the cost of hardware, while increasing the probability of an attack to a cage rather than an actual server. Each cage requires a dedicated network interface and has a unique IP address.

Intruders are permitted to attack the artificial system configuration and user data. Within the cages, intruders use the actual hardware, operating system, applications and file system. The logs, configuration, and other files related to the host software are located outside the cages, inaccessible to the intruder. Changes that intruders make to the file system affect the cages, but do not affect the underlying system.

Within the cages, chroot causes the cage home directory to appear as the system's root directory. The term chroot stands for change root. If anyone obtains access to the cages, they are contained within the cage root directory and cannot see or gain access to the real system's directories.

## Prevention, detection and response

Using Bruce Schneier's simple model of security, let's now look at how Symantec Decoy Server works with the concepts of prevention, detection and response.

## Prevention

The most common attacks use scripted or automated tools that hack into the system so that attackers do not have to analyze their targets. Hence, it is wise to secure the system with a firewall and strong authentication mechanisms. In the case of skilled attackers, who focus on targets of choice, deception and deterrence are the keys. Here, deploying a decoy as shield to cover unused ports of a production server can lure attackers away from actual production system and into the decoy server. When a hacker performs a port scan, the measure of prevention value is in deterring attackers so that they waste time and resources attacking a decoy server. Also, if an attacker is skilled, just knowing a decoy server is deployed could be a psychological weapon to scare him off.

## Detection

When looking at detection, it is clear that we already have a solution designed to monitor networks and detect malicious activity in Network Intrusion Detection Systems (NIDS). Yet, the solution is incomplete. Decoy server can add extensive value to detection. System administrators receiving alerts are often caught in a dizzying labyrinth of false positives, false negatives and aggregation data. In the midst of the chaos, many administrators are numbed and simply choose to ignore alerts or even turn off their intrusion detection systems. Decoy server, owing to its simplicity, addresses these challenges expertly.

Decoy server generally has no production traffic, therefore it is not prone to false positives in which the system alerts about valid production traffic. Also, decoy server addresses false negatives in that it detects system activity and not signatures which can miss new attacks. Additionally, decoy server aggregates very little data, yet this data is of extremely high value, and therefore easy to understand and diagnose.

## Response

Understanding the vulnerabilities in your system and how an attack happened, will lead the way in responding to break-ins and preventing similar future incidents. Decoy server addresses the challenges of preserving the integrity of data and may also be taken off-line in a crisis, unlike most high production systems which are polluted with high traffic and are essential to daily operations.

If it becomes necessary to use logs as evidence, the iButton acts as a digital credential, certifying the data has not been tampered with. You can verify the log records from the log viewer. See [“iButton”](#) on page 5.

## Content Generation Module (CGM)

The key to the realistic look and feel of a cage is the significant range and quantity of convincing content it contains. You can either install content such as software and sanitized files in the cage, or you can use the CGM to generate convincing content for the cage. Because the content is generated randomly, no two cages are the same.

The CGM generates the following types of content:

- A copy of the entire operating environment as it was installed on the host prior to installation of host software. Therefore any user accounts that exist on the host will be copied into the cage during the installation.
- Email messages generated from templates. Email templates can contain information specific to your site, such as your organization's official name, names of well known members of your organization, and your Internet domain name and network number. You supply these values during the installation.
- Home directories for each user that the software generates, as well as for each user name you provide to the administration console.

## Administration console

Symantec Decoy Server's Administration Console provides a remote interface from which you can edit the parameters for the hosts and cages, configure response and report policies, view the log data, replay cage sessions, and initiate a connection to the host machine using Secure Shell (SSH). Administration of Symantec Decoy Server is conducted through the UDP (User Datagram Protocol) port. The administrative port will not respond to TCP scans or probes.

The administration console allows you to configure automatic responses to Symantec Decoy Server events. To effectively and efficiently react to an attack, Symantec Decoy Server uses policy-based responses.

Filters within the response policies enable the administrator to eliminate false negative. Symantec Decoy Server can also send events to Symantec ManHunt™, enabling you to monitor Decoy Server and ManHunt events from a single console as well as configuring ManHunt responses to decoy server events.

For an additional level of event analysis, Symantec Decoy Server includes reporting capabilities. Reports can be generated and viewed immediately in the administration console, or they can be sent automatically on a scheduled basis.

## iButton

The iButton protects against falsification of log records and provides authenticated signatures to allow the log data to be used against an intruder. Each iButton has cryptographic circuitry and an engraved, guaranteed-unique registration number to authenticate the signature.



# Deploying Symantec Decoy Server

This chapter includes the following topics:

- [About deploying Symantec Decoy Server](#)
- [Getting started](#)
- [Deployment schemes](#)

## About deploying Symantec Decoy Server

When deploying Symantec Decoy Server, the placement of hosts and cages depends on the location and server types that Symantec Decoy Server will be protecting. The real server may be in front of or behind the firewall. It could be part of a cluster of servers that must be mirrored in its entirety in order to appear realistic to an attacker. You can use Symantec Decoy Server's Content Generation Module (CGM) to generate content, or you can customize your cage by installing any Solaris-compatible software.

## Getting started

The following are suggested steps to take before deploying cages within your network.

Before deploying cages within your network

- 1 Gather information on your existing network architecture and security policy. Discover where a high volume of traffic enters your network and where your trusted servers reside.
- 2 Learn the specifics of your applications. For example, if you have a cluster of Web servers, you may want to configure your cages to resemble Web servers, and then place them on the same network segment as your trusted Web servers.
- 3 Learn the specifics of your operating systems. Typically you would not want to place a cage, which resembles a UNIX server, in a cluster of NT servers.
- 4 After you survey your current network topology, strategically place cages throughout your network.

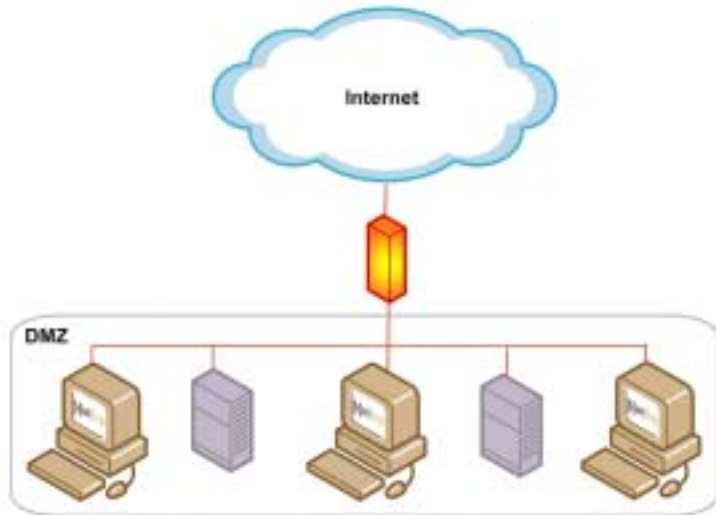
## Deployment schemes

You can use one of the following deployment schemes:

- [Minefield deployment scheme](#)
- [Honey Net deployment scheme](#)
- [Shield deployment scheme](#)
- [Custom deployment](#)

## Minefield deployment scheme

A common scheme for deploying Symantec Decoy Server systems is to place them among high-value targets.

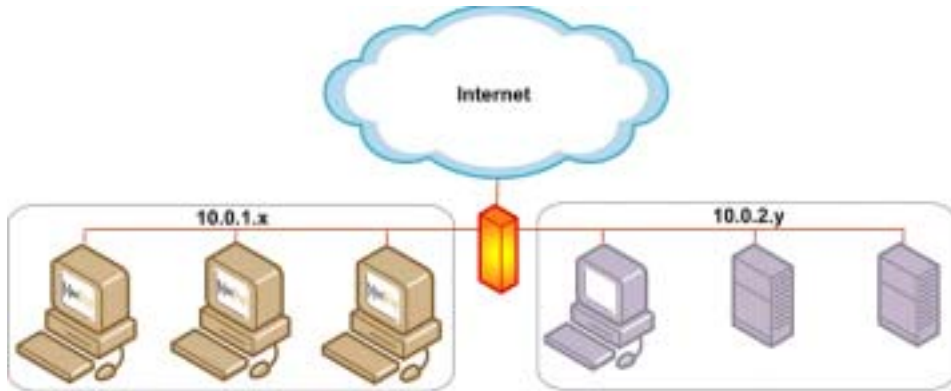


Minefield Deployment Scheme

The minefield deployment scheme reduces the probability of an attacker entering the actual trusted server. For example, if you deploy one Symantec Decoy Server for every three Web servers, someone attempting to gain access to the Web servers (by means other than HTTP) has a 25% chance of winding up in a cage. Additionally, configuring Symantec Decoy Server to be slightly more vulnerable than the actual servers increases the probability of an attacker targeting a cage.

## Honey Net deployment scheme

Typically a real network contains a cluster of servers, such as FTP, SMTP and HTTP servers.

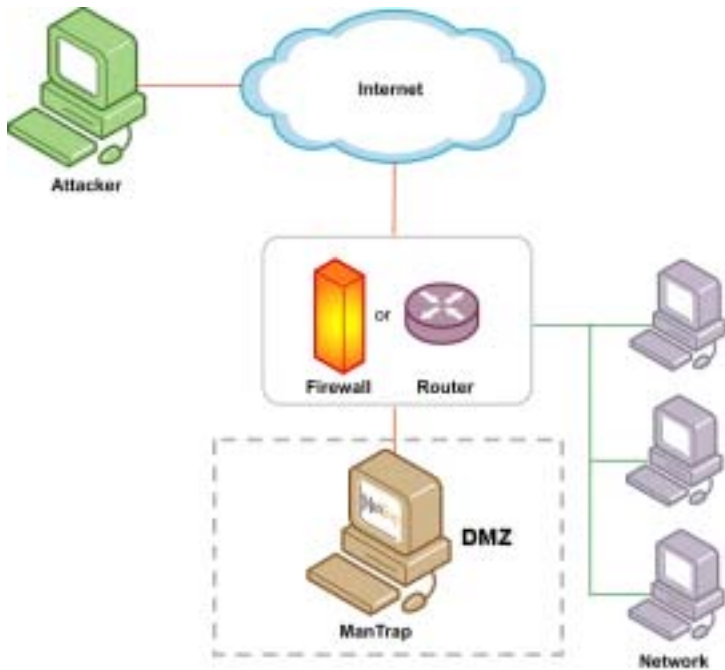


Honey Net Deployment Scheme

The honey net deployment replicates this cluster of servers by implementing an all-deception-host network, with the cages configured to resemble the actual servers and containing various applications to create a more realistic environment for the attacker. The purpose of such a deployment is to encourage the attacker to reveal his skill level and intentions, thereby allowing security administration efforts to focus on more serious threats. If you create a honey net deployment, set up rules in the redirection device to allow the attacker to only move within the honey net.

## Shield deployment scheme

The shield deployment scheme uses a redirection device to redirect attacks against high-value targets to Symantec Decoy Server.



Shield Deployment Scheme

For example, an attempt to connect to the public Web server through an un-permitted service, such as SMTP or telnet, is automatically redirected to a cage that mirrors the Web server but resides in a separate demilitarized zone (DMZ) to contain the attacker. You can configure the cages to replicate your public Web server so the attacker thinks he has made a successful attack.

## Custom deployment

You can customize your deployment to compliment your existing security policy.

Consider the following tips before deploying your cages:

- Place cages near critical servers to increase your chances of trapping an attacker where he is contained and his actions are monitored. Realize that, after an attacker successfully breaks into a single machine, he typically jumps

around to other machines within the network—whether for exploiting purposes or merely the challenge of compromising security.

- Assign the lowest IP addresses in a server pool to cages. When an attacker scans for available ports, often the ports on the lowest IP addresses within a server pool will register first. Assigning lower IP addresses within a network segment to cages increases the likelihood that the attacker will initially attack a cage.
- Configure your cages to be more vulnerable than your trusted systems. Attackers often target the servers that are easiest to exploit. Therefore, configure your cages to be more vulnerable than the trusted servers.
- Run popular applications or the same applications as your trusted servers inside the cages. You can add applications or files to make the system look more like the surrounding systems, or emulate the trusted server you think the attacker will exploit. Because Symantec Decoy Server is a real working system, it can run the applications necessary to make it appear as an internal or external Web, file, DNS, FTP, or other application server.

# Installing the Host Software

This chapter includes the following topics:

- [About installing the host software](#)
- [Getting started](#)
- [Installing Symantec Decoy Server](#)
- [Configuring Symantec Decoy Server](#)
- [Upgrading Symantec Decoy Server](#)
- [Symantec Decoy Server processes](#)

## About installing the host software

The host installer is a command line program that allows you to configure the host and each cage. When installing the host software, you have options to start with a completely new configuration or load an existing configuration from another host installation. See [“Creating a host configuration”](#) on page 23 and [“Loading an existing configuration”](#) on page 31.

You can also perform an upgrade from Symantec ManTrap 3.01 to Symantec Decoy Server 3.1, and a configuration checker can be run post-installation to report and fix any configuration errors. See [“Upgrading Symantec Decoy Server”](#) on page 34.

## Getting started

To ensure that the installation process goes smoothly

- 1 Obtain the following:
  - Network interface cards—one interface per cage plus one interface dedicated for the administration console
  - Solaris installation media
  - iButton (optional)  
See [“Choosing a token”](#) on page 20.
  - Symantec Decoy Server floppy disk, which contains a certification file that validates the iButton
  - Symantec Decoy Server installation CD
- 2 Determine the IP addresses and host names to assign to each cage.
- 3 Determine in which cages, if any, you want to enable Content Generation Module.
- 4 Determine the sizes to configure each cage. The host installer allows you to configure your server to replicate a:
  - 2, 4 or 9 gigabyte standard server,
  - 4 or 9 gigabyte mail server, or a
  - 9 gigabyte file server.

You are also given the option of customizing your cage to replicate another server or database. The total size of the cages will affect the disk space

requirements during the Solaris installation. See [“Installing Solaris”](#) on page 17.

- 5 Determine the host name to use for the host.
- 6 Choose the passphrase you want to use for the user “admin.”

## System requirements

The host software and administration console must be installed on separate machines. This section describes the system requirements for the host software and administration console.

### Host requirements

Requirements are as follows:

- **Hardware**—Sun Ultra 5 or greater
- **Processor**—Sun Hardware Compatibility List (HCL) certified Intel Pentium II or greater
- **Memory**—Minimum of 256 MB system memory (plus 128 MB for each additional cage).
- **Network Interfaces**—One Sun HCL certified network interface card per cage plus one supported network interface for the administration console. For example, a four cage system requires five network interfaces.
- **Hard Disk Drive Space**—2GB required for host software, plus minimum 2GB per cage

---

**Note:** Any software aside from the operating system installed into the cage increases minimum disk space requirements. If you plan to create a custom cage, ensure that you allocate sufficient disk space and that sufficient space is allocated to the partition in which you plan to install the host software. Also, when backing up the cage, the backup copy will be the exact size of the cage, so ensure that there is enough disk space on the partition for the cage copy.

---

- **Communication Port** (ttyb communication port)—if your SPARC machine has one physical DB25 port, a splitter is required that converts the one physical communication port into two communication ports.
- **Serial Port**—DB9 serial port or 9-pin adapter
- **Software**—Symantec Decoy Server supports the following software:

- Solaris 7 SPARC™ with full distribution and OEM support, patch level 106541-04 or higher
- Solaris 7 Intel® with full distribution, patch level 106542-04 or higher
- Solaris 8 (SPARC or Intel) 10/01 HCL or higher, with full distribution and OEM support
- **File System**—Symantec Decoy Server can only be installed on Solaris Unix File Systems (UFS).
- **Devices**—CD-ROM and floppy drives recommended

## Pre-installation

Before installing the host software, you must prepare the machine with the required hardware and software.

To prepare the machine for Symantec Decoy Server

- 1 Perform the initial installation of Solaris 7 or 8 with full distribution and OEM support on the host machine, and patch the machines to the supported level. See [“Installing Solaris”](#) on page 17.

---

**Note:** Ensure that there is sufficient disk space on the machine, and that sufficient space is allocated to the partition(s) where you plan to install cages. The cages are typically installed in /usr, and a minimum space of 2 gigabytes per cage is required. See [“Host requirements”](#) on page 15.

---

- 2 Verify the Solaris installation. See [“Verifying the Solaris installation”](#) on page 18.
- 3 Install the network interface cards. See [“Installing network interface cards”](#) on page 18.
- 4 Install the software or hardware token. See [“Installing Symantec Decoy Server”](#) on page 19.
- 5 Perform an initial installation of the Solaris operating system with full distribution and OEM support on the host machine; do not use an existing installation. See [“Installing Solaris”](#) on page 17.

After you configure and install the host software, you can install the administration console on a separate machine and set the host and cage parameters.

# Installing Solaris

You must perform an initial installation of the Solaris operating system with full distribution and OEM support on the host machine; do not use an existing installation. Patch the machine to the supported level. If you plan to install anything on the host machine aside from the Solaris operating system, ensure that there is sufficient disk space available on the partition(s) on which you intend to install the cages. Also be sure that enough of this space is allocated to each directory where you plan to install each cage. You can also install software inside or outside of the cage after you install the host software.

- **Swap Files**—Symantec Decoy Server does not support swap files, only swap partitions. As cages are denied access to the host file system, swap files which reside on the host file system, although configured, are not accessible to caged processes. Swap space must be configured to use swap partitions for Symantec Decoy Server to function properly.

---

**Warning:** We strongly recommend that you do not configure swap files during the Solaris installation.

---

- **Host User Accounts**—During the installation, all user accounts on the host are propagated into the cages. User accounts are necessary within the cage in order for you to establish cage sessions.

If you add the user accounts to the host before the installation, you do not have to add user accounts to each individual cage. All passwords (except for root) appear similarly in the cages as they do on the host. The root password must be set within each cage after the installation.

You can add user accounts with the UNIX `useradd` and `passwd` commands. The CGM also uses user accounts to maintain a mail server environment within the cage. To create an organization-specific mail server, custom user accounts can be added during the cage CGM configuration or on the host before the installation. The CGM is configured during the installation, and you can add users at that time.

In addition to the user accounts you can configure, the CGM integrates user accounts added to the host before the installation. The CGM will generate content for all users with user IDs between 1000 and 60,000.

You can add, change, or delete user accounts after the installation using the CGM utilities.

- **X Support**—Symantec Decoy Server does not support X in the cages. If an application you want to install in the cage requires X, you must use either X forwarding or SSH tunneling.

- **RPC Services**—If RPC services are running on the host, they are visible on all interfaces and allow RPC-based attacks access to the host. Therefore, we recommend that you do not run RPC outside the cages. Also note that running services, such as SSH, which by default bind to all interfaces on the host, means that this service may also be available on the cage interface. This may allow an attacker to gain access to the host rather than the cage. If you need to run such a service outside of the cage, be careful to configure it so that it only binds to the interface used for administration.
- **Operating System Upgrades**—The installation replicates the host's operating environment into each cage. Therefore, any update to the operating system on a host, such as an upgrade from Solaris 7 to Solaris 8, requires a full re-install of Symantec Decoy Server software.

---

**Warning:** Make a note of the host's IP address. You will need it to configure Symantec Decoy Server software in the administration console.

---

## Verifying the Solaris installation

Before installing Symantec Decoy Server software, Symantec recommends that you verify the Solaris installation with OEM support. Any errors in the Solaris installation will cause Symantec Decoy Server to function improperly.

To verify Solaris 7 and 8 with OEM support

- 1 Change directories by entering the following command:

```
# cd /var/sadm/system/admin/
```

- 2 View the CLUSTER by entering the following command:

```
# cat CLUSTER
```

- For SPARC editions, if `CLUSTER=SUNWCxall`, the entire installation was successful.
- For Intel editions, if `CLUSTER=SUNWCall`, the entire installation was successful.

If the installation was not successful, refer to the Solaris documentation. You may need to re-install Solaris.

## Installing network interface cards

The Symantec Decoy Server server requires a network interface for each cage and for the administration console.

---

**Note:** Symantec recommends that you install the host and cage on separate network segments.

---

Symantec Decoy Server is compatible with all Sun HCL-certified NICs.

Install the NICs in your system and verify the correct installation. Refer to the appropriate manual for installation and verification instructions.

## Using MAC addresses

A machine's Media Access Control (MAC) address is the hardware address of the interface that uniquely identifies each node of a network. For Symantec Decoy Server software to function properly, each network interface must have a unique MAC address. To ensure that you are using unique MAC addresses, use the MAC addresses assigned to the adapter's network interfaces.

To use the unique MAC addresses assigned to the adapter's network interface

- 1 Become root or the superuser and enter the following command to set the local mac address? variable to true:

```
# eeprom local-mac-address?=true
```

- 2 Enter the following command to validate the local-mac-address? variable is set to true:

```
# eeprom local-mac-address?
```

- 3 Restart the machine.

- 4 Enter the following command to validate unique MAC addresses:

```
# ifconfig -a
```

The following is an example of the 10-digit MAC address following the word ether:

```
ether 8:0:20:af:8c:51
```

## Installing Symantec Decoy Server

During the installation of Symantec Decoy Server 3.1, you can choose to sign log files with a software token or an iButton hardware token. If both exist on your system, the iButton is the default.

## Choosing a token

The main function of the software token is to provide basic log signing functionality with limited tamper protection. The hardware token known as the iButton is an optional, upgraded feature of Symantec Decoy Server 3.1. The iButton provides all of the benefits of the software token, plus these additional benefits:

- Provides a secure source for signing keys
- Provides a secure source for time stamps other than the machine clock
- Ensures that cryptographic services are off-loaded to a FIPS 140-1 hardware token (a secure module that is evaluated at high rigor levels), thus, preventing tampering with cryptographic routines

After you have decided whether to use a hardware token or a software token, you can proceed to install the token. See [“Installing a hardware token”](#) on page 20 or [“Installing a software token”](#) on page 21.

## Installing a hardware token

The iButton provides digital time-stamps to authenticate log records. The iButton comes installed in a 9-pin caddy and attaches to a 9-pin communication port. If the host machine does not have a DB9 communication port, install a 9-pin adapter.

---

**Warning:** If you are using a SPARC machine, do not plug the iButton into the primary (ttya) communication port if there is no keyboard on the system. Symantec Decoy Server will not function properly when the iButton is plugged into this port and no keyboard is present on the machine.

If your SPARC machine has one physical DB25 port, please check with Sun Microsystems to verify that your serial port can be split and, if so, then connect a splitter that converts the one physical communication port into two communication ports. Then plug the iButton into the secondary (ttyb) port.

If your SPARC machine has two communication ports, plug the iButton into the secondary (ttyb) communication port.

---

### To install the iButton

- 1 Plug the iButton caddy into the appropriate 9-pin communication port on the host machine.
- 2 Insert the token into the caddy.

- 3 Load the installation media into the floppy drive.  
See [“Loading the installation media”](#) on page 22.

## Disabling iButton

You can disable the iButton at any time, however, disabling the iButton will cause Symantec Decoy Server to cease using the iButton for log signing and log verification. This means that any logs that have been signed with the iButton will no longer be considered valid because the iButton is no longer in use. For this reason, Symantec recommends that you verify and compress the log database without running the cages; this preserves the history.

To disable iButton

- 1 Log into the Symantec Decoy Server as root.
- 2 Change to the Symantec Decoy Server configuration directory.  
This directory is located within the root decoy directory and is named etc.
- 3 Enter the following command:  

```
cd `cat /etc/rtihome/` /etc
```
- 4 Edit the host configuration file (rti.conf) by changing the value of the HAVEIBUTTON configuration parameter from 1 to 0.
- 5 Reboot the host to allow the configuration change to take effect.
- 6 Remove the iButton caddy from the DB9 port.

## Installing a software token

If you have selected to install Symantec Decoy Server with a software token.

---

**Note:** Before adding a software token, you must first disable a hardware (default) token, if you have one. See [“Disabling iButton”](#) on page 21.

---

To install Symantec Decoy Server with a software token

- Load the installation media.  
See [“Loading the installation media”](#) on page 22.

## Loading the installation media

Loading the Symantec Decoy Server installation media prepares you to begin a new configuration, load an existing configuration file, and/or upgrade from Symantec ManTrap 3.01 to Symantec Decoy Server 3.1.

To load the installation media

- 1 Enter the following to verify that a previous floppy is not mounted:  

```
# eject floppy
```

  - If you are installing a hardware token, insert the Symantec Decoy Server floppy disk in the floppy drive and place the Symantec Decoy Server CD into the CD-ROM drive.
- 2 Change to the CD-ROM Symantec Decoy Server directory, typically /cdrom/cdrom0.  

```
# cd /cdrom/cdrom0
```
- 3 Enter the following command to run the host installer:  

```
# ./Install
```
- 4 Enter 'yes' to agree to the terms of the Symantec Decoy Server End User License Agreement.
- 5 Select an option below:
  - Enter 1 to load an existing configuration file.  
See [“Loading an existing configuration”](#) on page 31.
  - Enter 2 to upgrade from Symantec ManTrap 3.01 to Symantec Decoy Server 3.1.
  - Enter 3 to begin a new configuration.  
See [“Creating a host configuration”](#) on page 23.

## Configuring Symantec Decoy Server

If this is your first installation, or if you want to create a new host software configuration, the installation procedures discussed in the following sections will provide guidance:

- [Creating a host configuration](#)
- [Creating a cage configuration](#)
- [Installing host and cage configuration values](#)

- [Loading an existing configuration](#)
- [Upgrading Symantec Decoy Server](#)
- [Auto-installation](#)
- [Remote installation](#)
- [Uninstalling Symantec Decoy Server](#)
- [Starting and stopping Symantec Decoy Server](#)
- [Upgrading Symantec Decoy Server](#)

---

**Note:** The host software takes approximately one hour per cage to load. Allocate sufficient time to install the software.

---

## Creating a host configuration

This section describes the host configuration portion of the installation process.

To create and install a new host configuration

- 1 Enter the absolute path, including the filename, to save the configuration file.
  - Press Enter to accept the default path, typically /etc/mt3.install.  
You can use this configuration for future installations. See [“Loading an existing configuration”](#) on page 31.
- 2 When asked if you have a valid iButton installed on the machine:
  - Select 1 and press Enter to choose Yes, then proceed to step 3.
  - Select 2 and press Enter to choose No, then proceed to step 5.  
The software token and certificate are generated.
- 3 Enter the path to the iButton certificate.
  - Press Enter to accept the default path, typically /floppy/floppy0.
- 4 Enter the path to the iButton device.
  - Press Enter to accept the default path, typically /dev/ttyb.  
Symantec Decoy Server will install the iButton. If there is a problem installing the iButton, an error message will appear. If you are still having problems.

---

**Note:** The soft token is installed after the hardware token in the eventuality that it becomes necessary to support iButtonless functions later.

---

- 5 Enter the Symantec Decoy Server host install path.  
Symantec Decoy Server creates a directory in the specified install path in which all host files are written.
  - Press Enter to accept the default, typically /usr.
- 6 Enter the host default router address.
  - Press Enter to accept the default router IP address, which is typically located in the directory /etc/defaultrouter.
- 7 Enter Yes or No to automatically compress the Symantec Decoy Server database when it grows too large.
- 8 Enter the maximum age of a database record (in days) before the database will automatically remove it (enter 0 to disable automatic removal).
- 9 Enter Yes or No to select whether or not to keep a backup of trimmed database records.
- 10 Choose an admin passphrase and press Enter.  
The passphrase can be between 8 and 256 characters in length and is case sensitive. There are no restrictions on the type of characters the passphrase can contain. For optimal security, the passphrase should consist of at least one number, both upper and lower case letters, and at least one punctuation character.

---

**Note:** Symantec Decoy Server automatically creates an “admin” account on the host.

---

- 11 Re-enter the admin passphrase and press Enter.

---

**Note:** Make a note of this passphrase—you must use it to access the host from the administration console.

---

- 12 Enter the admin port.
  - Press Enter to accept the default, typically 12387.

---

**Note:** The host installer will report the number of network devices available for cages.

---

- 13 When asked if you would like to configure additional network interfaces:

- Select 1 and press Enter to choose Yes.
  - Select 2 and press Enter to choose No, and proceed to step 12.
- 14 Enter the number of additional network devices you want to configure and press Enter.  
For each of the additional network devices, perform the following steps:
- Enter the name of the network device.  
Follow the naming convention of the network interface card, for example, iprb3.
  - Enter an IP address for the network interface.  
This will be the cage IP address.
  - Enter a netmask for the network interface.  
Symantec Decoy Server will attempt to configure the network interface.  
This may take a few seconds.
- 15 Select an administrative network device.  
This is the network interface used to communicate with the administration console, typically hme0 on a SPARC machine or e1x10 on an Intel machine.
- 16 Select the number of cages you wish to configure and press Enter.  
You can configure between 1 and 4 cages, based upon the number of available network devices you have and the number of cages you purchased with the product license.

---

**Note:** The host installer will report the number of network devices available for cages.

---

- 17 The values you entered during the host configuration display, and you are asked if you would like to change any of these values.
- Select 1 and press Enter to choose Yes.
  - Select 2 and press Enter to choose No.

---

**Note:** Symantec Decoy Server will calculate directory sizes for each cage. This may take a few minutes.

---

See [“Creating a cage configuration”](#) on page 25.

## Creating a cage configuration

This section describes the cage configuration portion of the installation process. Perform these steps for each cage you want to configure.

To create and install a new cage configuration

- 1 Enter a cage hostname, typically the network name assigned to the cage.
- 2 Enter a cage install path.  
Symantec Decoy Server will create a cage# directory in the specified install path in which all cage files will be written. For example, if you accept the default directory, /usr/decoy, Symantec Decoy Server will install the cage files in /usr/decoy/cage1.
- 3 Select a cage network device from the list of available network devices.
- 4 Select whether or not you want to use the mountpoints configuration of a previous cage to determine the configuration to lay out the cage directory architecture. See [“Mount points configuration”](#) on page 29.
  - If you want to use a mountpoints configuration of a previous cage, select the cage and proceed to step 5.
  - If this is your first cage configuration or you want a new mount points configurations, select 1 and press Enter for No.
- 5 Select a predefined 2, 4 or 9 GB mountpoints option, or select Custom and press Enter.  
If you select Custom, follow these steps to customize the partition sizes of the cage.
  - Enter the number of mountpoints you want to configure and press Enter. The root partition (/) will automatically be added.
  - For each mountpoint you want to add, enter a mountpoint path and press Enter.
  - For each mountpoint you specified, enter a mountpoint size in megabytes and press Enter. Do not enter a size smaller than the listed minimum size.

---

**Note:** The size of all mount paths add up to the total size for the cage. Be sure to allocate sufficient disk space for each cage. See [“Host requirements”](#) on page 15.

---

The installer lists “Automatic Copies,” that is, the directories that are automatically copied into the cage. This list cannot be edited, however, you can specify Custom Copies to copy other directories to the cage, in addition to those that are automatically created.

If this is not your first cage installation, default values from the previous cage appear in the Custom Copies option.

- 6 Enter an absolute path to the directories to copy in the form /directory, and separate the directories with a colon. You must not separate the entries with spaces.
  - If you do not want to create any additional directories, simply press Enter to skip this step.
  - If you do not want to copy directories into the cage, enter NONE and press Enter.

---

**Note:** You cannot add directories that are automatically excluded from the cage.

---

The installer lists “Automatic Excludes”, that is, the directories that are automatically excluded from the cage. Symantec Decoy Server automatically excludes the cage install path, which is /usr/decoy by default. This list can not be edited, however, you can specify Custom Excludes to exclude other directories from the cage.

- 7 Enter an absolute path to the directories to exclude in the form /directory and separate each directory with a colon.  
You must not separate the entries with spaces.
  - If you do not want to exclude any additional directories, simply press Enter to skip this step.

---

**Note:** The host installer will not automatically exclude remotely mounted file systems. Be sure to exclude all remote file systems that you do not want copied into the cage. For example, if you execute the host installer from a remote file system, exclude the location of the host installer.

Exclude all NFS mounted directories from the cage. If an NFS mounted directory is imported into a cage, the install may run out of space as it will be unable to correctly calculate the final installed size of the cages.

---

- 8 Enter a decoy network interface.  
This is not the actual network interface the cage is on, but the one presented to the intruder inside the cage.
- 9 Enter the absolute path to the cage failover log location.  
This is the location where the logs are written in the case of log database failure.
- 10 Enter the decoy default router.  
This is not the actual default router, but the one presented to the intruder inside the cage.

---

**Note:** The decoy default router must be a real machine in order to maintain a realistic cage environment.

---

- 11 Enter the cage log file path; used to backup the cage in case of database failure.
- 12 Enter the cage default route; this is the IP address of the cage.
- 13 Select if you want to enable content generation.  
The Content Generation Module (CGM) creates a mail server customized to your organization based on your entries in the administration console.  
See “[Content Generation Module \(CGM\)](#)” on page 4.
  - Select 1 and press Enter to choose Yes.
  - Select 2 and press Enter to choose No, then skip to step 23.

---

**Note:** The CGM creates content for the cage in English only, therefore, you must select No for non-English versions of Solaris.

---

- 14 Select if you want to use the CGM of a previous cage.
  - Select the cage number and press Enter to use a previous cage’s CGM.
  - Select No and press Enter to run the CGM.
- 15 Enter the organization or company name that the CGM will integrate into the cage data files in order to create an environment that appears realistic to an intruder.
- 16 Enter the domain name that the CGM appends to the end of user email addresses.  
Although you can supply a fictitious value for the domain name, the data generated for the cage will appear more realistic if you enter your company’s actual domain name.
- 17 Enter the host name that the CGM uses to configure the scripts that it places inside the cage.  
The name should be different from the host machine.
- 18 Enter the number of randomly created user accounts you want to add to the cage.  
The CGM generates random user accounts that it uses to construct data files for the cage.
- 19 Enter the full name of the user, for predefined users such as executives.

This allows you to increase the realistic appearance of the cage without revealing sensitive information about your company. You can add up to five user accounts.

**20** Enter the login name of the user.

The login name can consist of up to eight alphanumeric characters and must not include spaces.

**21** Select the gender of the user.

- Select 1 and press Enter for a male.
- Select 2 and press Enter for a female.

**22** Repeat the previous three steps for each user account you want to add.

**23** Select whether or not you want to back up the cage.

---

**Warning:** Choosing to backup cages doubles the free disk space requirements, so ensure that there is enough disk space on the partition for the cage copy.

---

- Select 1 and press Enter to choose Yes, then enter the directory path for the backup copy.
- Select 2 and press Enter to choose No.  
The values you entered during the cage configuration display.

**24** Select whether or not you want to change any of the cage values.

- Select 1 and press Enter to choose Yes.
- Select 2 and press Enter to choose No.

Repeat steps 1 through 24 to configure each cage.

**25** Select whether or not you want to run the CheckConfig script before you reboot the system; this utility checks the setup for many common configuration problems.

- Select 1 and press Enter to choose Yes.
- Select 2 and press Enter to choose No.

## Mount points configuration

Symantec Decoy Server allows you to configure each cage with a unique partition layout. You can use Symantec Decoy Server's predefined mount points configuration options, or you can customize the mount points configuration, described below:

- **2-gig**—This configuration represents a standard 2GB server. The /usr/ directory is typically larger than the other directories in a standard drive.
- **4-gig**—This configuration represents a standard 4GB server. The /usr/ directory is typically larger than the other directories in a standard drive.
- **4-gig mailserver**—This configuration represents a 4GB standard mailserver. In a standard mailserver, the /var/ directory is usually larger than the other directories because the mail pool is typically stored in the /var/ directory.
- **9-gig**—This configuration represents a standard 9GB server. The /usr/ directory is typically larger than the other directories in a standard drive.
- **9-gig mailserver**—This configuration represents a standard 9GB mailserver. In a standard mailserver, the /var/ directory is usually larger than the other directories because the mail pool is typically stored in the /var/ directory.
- **9-gig filesaver**—This configuration represents a 9GB server that is used specifically for sharing files over NFS. Therefore the /export/ directory is larger than other directories in a standard server.

## Installing host and cage configuration values

This section describes the installation portion of the installation process.

To install host and cage configuration values

- 1 Select **Begin install** to install Symantec Decoy Server with the current configuration.
  - If you already have Java Runtime Environment (JRE) v.1.4 running on the host machine, enter **No** and enter the path to the java binary, which is by default /usr/local/jre.
  - If you do not have JRE v.1.4 running on the system, enter **Yes** to install it, then enter the JRE install path and press **Enter** to accept the default install path, /usr/local/jre.  
When JRE license agreement appears, enter **Yes** to agree with the terms and proceed with the Symantec Decoy Server and JRE installation.

---

**Warning:** Cage installation takes approximately one hour per cage. Restart the system when prompted. Do not reconfigure the disks, swap files, or memory after the installation.

---

- 2 When the installation is complete, you are prompted to reboot your machine.
  - Restart your machine using the `init 0` command instead of the `reboot` command to “cleanly” shutdown Symantec Decoy Server.
- 3 The next step is to install the administration console.

## Loading an existing configuration

You can load, edit and install any existing configuration at any time. See [“Creating a host configuration”](#) on page 23 and [“Creating a cage configuration”](#) on page 25.

To load an existing configuration

- 1 Load the Symantec Decoy Server CD and floppy.
- 2 Run the host installer and select option 1 to load an existing configuration file. See [“Loading the installation media”](#) on page 22.
- 3 Enter the absolute path, including the file name, of the host configuration file and press Enter.
- 4 Select if you have a valid iButton installed on the machine:
  - Select 1 and press Enter to choose Yes.
  - Select 2 and press Enter to choose No.
- 5 Select if you would you like to begin installation or modify configuration values.
  - Select 1 and press Enter to Begin Installation.
  - Select 2 and press Enter to choose Modify Values.
- 6 Enter the administrative passphrase.
- 7 Select whether or not you want to run the CheckConfig script before you reboot the system; this utility checks the setup for many common configuration problems.
  - Select 1 and press Enter to choose Yes.
  - Select 2 and press Enter to choose No.

## Auto-installation

If you want to re-install the Symantec Decoy Server with the same configuration values as the initial install, you can perform an automatic installation. This allows

you to quickly install Symantec Decoy Server without editing the host or cage configuration values. See [“Loading an existing configuration”](#) on page 31.

To auto-install Symantec Decoy Server

- 1 Enter the following to verify that a previous floppy is not mounted:  

```
# eject floppy
```
- 2 Insert the Symantec Decoy Server floppy disk in the floppy drive and place the Symantec Decoy Server CD into the CD-ROM drive.
- 3 Assuming volume management is running, enter the command:  

```
# volcheck -v
```
- 4 Change to the CD-ROM Symantec Decoy Server directory, typically /cdrom/cdrom0.  

```
# cd /cdrom/cdrom0
```
- 5 Enter the following command to run the auto-install script:
  - If you are using an iButton run:  

```
# ./Install -auto <mt options file> <iButton cert path>  
<iButton device> [<admin passphrase>]
```
  - If you are not using an iButton run:  

```
# ./Install -autonoib <mt options file> [<admin passphrase>]
```

**<mt options file>**—The absolute path to the saved configuration file. If you saved this in the default location, the file name is /etc/mt3.install.

**<iButton cert path>**—The path to the iButton certificate file, typically /floppy/floppy0.

**<iButton device>**—The communication port to which the iButton is attached. If you are installing on a SPARC machine, the iButton device is typically /dev/ttyb.

**[<admin passphrase>]**—The passphrase for the “admin” account. The passphrase must be at least 8 characters long. If you do not specify a passphrase on the autoinstall command line, you will be prompted for one.

## Remote installation

To install to a remote host

- 1 Insert the Symantec Decoy Server installation CD into the local machine's CD-ROM drive.
- 2 Tar the Symantec Decoy Server installation CD contents. The following example uses the CD-ROM directory /cdrom/cdrom0:

```
# tar -cvf mtinstall.tar /cdrom/cdrom0/<platform>
```

where <platform> is the location of the platform specific files you wish to install on your remote host. The CD-ROM is set up with a directory for each platform on which you can install Symantec Decoy Server.

- 3 SCP the tarball to the host machine.

```
# scp ./mtinstall.tar <user@host>
```

- 4 SSH to the host machine.

```
# ssh <user@host>
```

---

**Note:** SCP and SSH will require an implementation of SSHD running on your host machine.

---

- 5 Untar the mtinstall.tar file.

```
# tar -xvf mtinstall.tar
```

You can now proceed with the host installation. See [“Installing host and cage configuration values”](#) on page 30.

## Uninstalling Symantec Decoy Server

If you want to uninstall Symantec Decoy Server, follow the instructions below.

To uninstall Symantec Decoy Server

- 1 Change to the <rti\_home>/bin directory, which is by default /usr/decoy/bin.

```
# cd /usr/decoy/bin
```

- 2 Execute the uninstall script.

```
# ./uninstall.sh
```

A confirmation question appears.

- 3 Enter Yes to uninstall Symantec Decoy Server.
- 4 Restart the machine when prompted. Symantec Decoy Server and all of its components will be removed.

## Starting and stopping Symantec Decoy Server

The installation process adds startup scripts to the “rc” directories to automatically load the host and cages upon booting the host machine. To start Symantec Decoy Server, simply start the host machine.

To stop Symantec Decoy Server, preform one of the following

- Upon restarting the machine, Symantec Decoy Server will display a process number. To stop Symantec Decoy Server from loading, run:

```
kill <process #>, or
```

- Rename the host startup script /etc/rc3.d/S99decoy to:

```
/etc/rc3.d/K99decoy
```

Restart the host machine. Symantec Decoy Server will not start after the system restarts. If you rename the host startup script to stop Symantec Decoy Server, you can either change the name back to /etc/rc3.d/S99decoy and restart the host machine or run:

```
/etc/rc3.d/K99 start (as the root user to start)
```

## Upgrading Symantec Decoy Server

If you plan to upgrade from Symantec ManTrap 1.6.1 (or lower) to Symantec Decoy Server 3.1, you must perform a completely new installation. See [“Installing Symantec Decoy Server”](#) on page 19.

If you plan to upgrade from Symantec ManTrap 2.x to Symantec Decoy Server 3.1, you must first upgrade to Symantec ManTrap 3.0, then follow these steps. See the *Symantec ManTrap Installation and Administration Guide, Version 3.0* for instructions on upgrading to Symantec ManTrap 3.0.

If you plan to upgrade from Symantec ManTrap 3.0 or 3.01 to Symantec Decoy Server 3.1, then follow these steps.

Upgrading to Symantec Decoy Server allows you to preserve your existing configuration.

---

**Warning:** If you are upgrading from Symantec ManTrap to Symantec Decoy Server, you will experience a break in functionality if you do not activate the license before installing the upgrade. It is very important in this case that you activate the license file first, then follow the upgrade process. See [“Activating a license”](#) on page 54.

---

To upgrade to Symantec Decoy Server

- 1 Enter the following to verify that a previous floppy is not mounted:

```
# eject floppy
```

- 2 Insert the Symantec Decoy Server floppy disk in the floppy drive and place the Symantec Decoy Server CD into the CD-ROM drive.

- 3 Change to the CD-ROM Symantec Decoy Server directory, typically /cdrom/cdrom0.  

```
# cd /cdrom/cdrom0
```
- 4 Enter the following command to run the host installer:  

```
# ./Install
```
- 5 Enter 2 to upgrade Symantec Decoy Server. The installer will prompt you for a set of configuration values.
- 6 Follow the installation steps.

## Symantec Decoy Server processes

The Symantec Decoy Server host software includes the processes that run outside the cages, as well as the cages themselves. The host software also includes the optional Content Generation Module (CGM), which creates the cage content presented to intruders. See [“Content Generation Module \(CGM\)”](#) on page 4.

### Host processes

Host processes are described below:

- **rti.ibuttond**—Daemon that monitors License and iButton activity, such as reporting impending license expiration, checkpoints, and iButton errors
- **rti.logd**—Host logging daemon that handles log failover and time stamping of messages
- **logdb**—Main logging database daemon
- **cagemand**—The cage manager that starts, stops, and monitors cage processes to maintain a stable environment
- **rti.conf**d—Configuration daemon that manages configuration files and changes.
- **rti.admind**—Administrative daemon that causes actions to occur on the host in response to administration console activity
- **rti.stealthd**—Administrative daemon that manages communication between the administration console and the host

### Cage processes

Cage processes are described below:

- **startcage**—Main cage process that appears as init inside the cage

- **rti.logd**—Cage logging daemon that receives log messages from cage sources and passes them onto the logging db  
It also handles log failover and time stamping.
- **rti.klogd**—Kernel logger daemon that logs messages from kernel modules
- **rti.maild**—Part of the CGM (Content Generation Module) that creates and deletes mail for users in the cage's roster file with UID's over 1000
- **rti.sniffd**—Network sniffer that processes all traffic that is received by the cage. Normally, this is only traffic to and from the cage, however, if the cage interface is placed into promiscuous mode the network sniffer will process all traffic on the local segment.

## Content generation system tools

The following processes are CGM system tools:

- **rti.makeuser**—Utility that adds employee entries to the new user file

---

**Note:** The roster file keeps track of all the cage users that the CGM knows about. The new user file is a roster of employees waiting to be added to the roster file. They will be added to the roster file the next time **rti.usergen** is run.

---

- **rti.newusers**—Utility lists the users in the new user file.
- **rti.deluser**—Utility deletes specified accounts from the roster file and the cages `/etc/passwd` and `/etc/shadow` files  
The cage's `/etc/passwd` and `/etc/shadow` files won't change until after restarting the cage.

---

**Note:** **rti.deluser** will not delete the user's home directory from the cage.

---

- **rti.usergen**—Utility that adds users to the roster file  
During installation with the `rerun` flag set to false, it will copy users from the hosts `/etc/passwd` file and will create a brand new roster file. When the `rerun` flag is set to true, it will append new users to the existing roster file, or create a new one if it does not exist.  
In either case it will randomly generate the specified number of users, merge in all users in the new user file (created by **rti.makeuser**), add them to the cage's `/etc/passwd` and `/etc/shadow` files and add them to the roster file.
- **rti.listuser**—Utility that lists the users in the roster file.

# Installing the Administration Console

This chapter includes the following topics:

- [About installing the administration console](#)
- [Installing the administration console](#)
- [Adding local accounts](#)
- [Adding host connections](#)
- [Adding user accounts](#)

## About installing the administration console

The administration console allows individual users to remotely monitor and administer hosts and cages from their local accounts.

To begin, Symantec Decoy Server automatically creates an “admin” account on the host during the host installation process to allow administrators access to the host. Respectively, to gain access to the host the Administrator must know the host IP address, port number, and passphrase entered during the host installation process.

Administrators may then configure user accounts that allow varying levels of access to the host, depending on the grouping: Operator, Manager, or Administrator.

## Installing the administration console

Install the administration console on a separate machine than the one containing the host software. You can install the administration console on either a Windows or Solaris machine. Be sure to follow the set of installation instructions corresponding to the type of installation you want to perform.

### System requirements

Install the administration console and host software on separate machines. You can install the administration console on a Windows® or UNIX® Solaris machine.

#### Windows

Requirements are as follows:

- Microsoft® Windows 98, NT® 4.0 or 2000/XP
- Pentium II or faster processor
- Minimum 128 MB RAM
- Minimum 5 MB free disk space
- Java 2 Runtime Environment 1.4 or higher

---

**Note:** If you do not have Java 2 Runtime Environment 1.4 installed on the console machine, you can install it from the Symantec Decoy Server CD.

---

## Solaris/Intel or SPARC

Requirements are as follows:

- Solaris 7 or 8/Intel or SPARC
- Minimum 128 MB RAM
- Minimum 20 MB free disk space

## Installing the administration console on Windows

The administration console requires Java™ 2 Runtime Environment (JRE) v. 1.4 or higher. The administration console installation process installs a JRE in the specified directory.

To install the administration console on a Windows

- 1 Place the Symantec Decoy Server CD in the CD-ROM drive.
- 2 Double-click **mtsetup.exe** in the CD-ROM.  
The Welcome dialog box appears.
- 3 Click **Next**.  
The License Agreement dialog box appears.
- 4 Read the license agreement, and click **Yes** to accept.  
The Choose Install Folder dialog box appears.
- 5 Click **Next** to install the administration console in the default directory.
  - Click **Browse** to select a different location.
- 6 Click **Next**.  
The Select Components dialog box appears.
- 7 Select Symantec Decoy Server Console and JRE and click **Next**.  
The Ready to Install dialog box appears.
- 8 Click **Next** to install the administration console and the JRE.  
The JRE license agreement appears.
- 9 Read the license agreement, and click **Yes** to accept.  
The Choose Destination Location dialog box appears.
- 10 Click **Next** to install the JRE in the default directory.
  - Click **Browse** to select a different directory.
- 11 Click **Next**.  
The Last Minute Notes dialog box appears.

- 12 Read the administration console README, and click **Next**.

The administration console and the JRE will be installed into the specified directories. The Installation Complete dialog box appears when the installation process is complete.

- 13 Click **Close**.

Now that you have finished installing both the host and the administration console, start the administration console and set the system parameters.

See “[Starting and stopping the administration console](#)” on page 41.

## Installing the administration console on Solaris

The administration console requires Java 2 Runtime Environment (JRE) v. 1.4 or higher. The administration console installation process installs a JRE in the specified install path.

To install the administration console and JRE on a Solaris

- 1 Place the CD into the CD-ROM drive and enter the following command to change to the CD-ROM directory:

```
# cd /cdrom/cdrom0
```

- 2 Enter the following command to run the administration console install script:

```
# ./InstallGUI
```

- 3 When prompted, enter install paths for the administration console, <gui\_path>, the administration console configuration files, and the JRE, <JRE\_path>.

- Press **Enter** to accept the default directories.

The Binary License Agreement text is displayed.

- 4 Press the space bar to scroll through and read the rest of the license agreement, and enter “YES” when asked to agree to its terms.

- 5 Allow the installation process to finish.

Then go to: <http://java.sun.com/j2se/1.4/install-solaris-patches.html#where>, and <http://java.sun.com/j2se/1.4/font-requirements.html> to download the recommended patches.

- 6 Install the patches.
- 7 Restart the machine when prompted.

Now that you have finished installing both the host and the administration console, start the administration console. See [“Starting and stopping the administration console”](#) on page 41.

## Uninstalling the administration console

To uninstall the administration console on a Windows system

- ◆ Select **Start > Programs > Symantec Decoy Server Admin Console > Remove Symantec Decoy Server Admin Console** program.

To uninstall the administration console on a Solaris system

- ◆ Delete all the contents in the `<gui_home>` directory.

## Starting and stopping the administration console

You can start or stop the administration console from either a Windows or a Solaris machine.

### Windows

To start the administration console from a Windows machine

- ◆ Go to the administration console location and select **Symantec Decoy Server Administration Console**. The Login dialog box appears.

If you are logging into the administration console for the first time, you must add a local account.

To stop the administration console

- 1 Select **File > Quit**.  
A confirmation dialog box appears to ask if you want to quit.
- 2 Click **Yes**.

### Solaris

To start the administration console from a Solaris machine

- ◆ Run the JRE with the `mtadmin` file to start the administration console.  

```
# <gui_path>/mtadmin
```

## Adding local accounts

Each user can create a local account with a unique user name and password to log into the administration console.

To add a local administration console account

- 1 Launch the Symantec Decoy Server Login dialog box.
- 2 Enter a new passphrase, and the new passphrase for confirmation.  
The passphrase must be at least 8 characters in length and contain a mixture of character types.
- 3 Click OK.  
See [“Changing the passphrase”](#) on page 42.

## Changing the passphrase

We recommend that you change the administrative password for your local account from time to time. Create a new passphrase; at least 8 characters in length and containing a mixture of character types.

To change your local account passphrase

- 1 Select **File > Change GUI Passphrase**.
- 2 Enter the old host passphrase, the new passphrase, and the new passphrase for confirmation.
- 3 Click OK.
- 4 Log into the administration console with your new passphrase.

## Adding host connections

The left pane of the administration console is empty the first time you log into the administration console. To monitor hosts and cages, you must add hosts to the account. The left pane then displays an administration tree listing all the hosts added to the local account.

If you are not an administrator for the host, a user account must be added before you can add the host connection.

To add a host connection for a local account

**1 Go to File > Add Host.**

The Host Configuration dialog box appears.

---

**Note:** If you are editing the host connection, you must first use the Host menu to Disconnect from and Edit the Host, respectively. See [“Disconnecting from hosts”](#) on page 47.

---

**2 Enter or edit the following parameters:**

- **Address**—The Symantec Decoy Server host name or IP address.
- **Stealth Port (UDP)**—The administration console listens to the host using the connectionless UDP port. Once a connection request is made, the stealthd daemon on the host tells the administration console the QSP or SSH port number to use. By default, the host software installation process sets the Stealth Port number to 12387. Do not change the port number at this time. You can change the port on which the administration console listens by changing the Stealth Port parameter on the host and in the administration console. See [“Connecting to the host using SSH”](#) on page 48.
- **QSP Port (TCP)**—QSP, or query service proxy is the proxy the host uses to communicate with the administration console and the log database. You may want to define a QSP Port value in order to pass through a firewall that is blocking ports.  
Checking Random will allow you to better hide from portscans.
- **SSH Port (TCP)**—The SSH port is used when you SSH into the host from the administration console. You may want to define an SSH Port value in order to pass through a firewall that is blocking ports.  
Checking Random will allow you to better hide from portscans.
- **User**—The user name for your account.  
If you have the host “admin” account, enter admin as the user name. The admin host account was created during the installation.  
If you have a host Operator, Manager, or Administrator account, enter the user name that the administrator entered when adding the user account.
- **Passphrase**—The passphrase for your account. An icon with the host name and IP address appears in the administration tree. See [“Host status icons”](#) on page 45.  
If you have the host “admin” account, enter the administration passphrase for the host that was entered during the host installation.

If you have a host Operator, Manager, or Administrator account, enter the passphrase that the administrator entered when adding the user account.

**3 Click OK.**

You can now log on to the host. However, you must repeat these steps for each host you have permission to add to your local account.

## Connecting to hosts

You must connect to the host in order to administer or monitor the host and view cages. See [“Viewing cages”](#) on page 45.

To connect to hosts from the administration console

- ◆ Click the icon of the host you want to connect to and select **Host > Connect**.

To connect to all hosts in your administration tree at once

- ◆ Select **File > Connect All**.

---






**Note:** The first connection may take a few seconds as the administration console must initialize the stealth protocol for the first connection.

---

## Host status icons

The following table describes the host status icons:

Table 4-1 Host Status Icons

Icon	Description
	The host has been added to the account, but the administration console is not connected to the host. See <a href="#">“Disconnecting from hosts”</a> on page 47.
	The administration console is attempting to connect to the host.
	A Critical event has occurred in a cage within the past 1 hour.
	A Suspicious event has occurred in a cage within the past 1 hour.
	An Important event has occurred in a cage within the past 1 hour.

## Getting host information

When connected to a host you can get information on the host operating system, Symantec Decoy Server version number, and disk usage by clicking **Get Host Info...** in the **Host** menu.

## Viewing cages

You must connect to the host in order to administer or monitor the host and view cages.

To view cages

- ◆ Double-click the host icon to view the cage status icons labeled for each cage on the host. See [“Cage status icons”](#) on page 46.

- To refresh the cage status
- ◆ Select **Cage > Reset Health**.

Cage status icons

The following table describes the cage status icons:

Table 4-2           Cage Status Icons









Icon	Description
	The cage has been added to the account, but the administration console is not connected to the host.
	A Critical event has occurred in a cage within the past 1 hour.
	A Suspicious event has occurred in a cage within the past 1 hour.
	An Important event has occurred in a cage within the past 1 hour.
	The cage has been stopped.
	The cage has crashed.
	The status of the cage is unknown.
	The cage is busy backing up or loading files.

Table 4-2 Cage Status Icons

Icon	Description
	The cage is unlicensed.

## Disconnecting from hosts

You may want to disconnect from the host if another administrator wants to manage the same host.

To disconnect from hosts

- ◆ Click the icon of the host you want to disconnect and select **Host > Disconnect**.

To disconnect from all hosts

- ◆ Select **File > Disconnect All**.

## Deleting host connections

The administration tree on the left side of the administration console lists the hosts that you added to your local account. You can delete hosts if you no longer want to administer them from your local account.

---

**Note:** Deleting a host from your account does not uninstall the host software.

---

To delete hosts from a local account

- 1 In the administration tree, select the icon of the host you want to remove.
- 2 Select **Host > Delete**.  
A confirmation dialog box appears.
- 3 Click **Yes**.  
The host can no longer be administered from your account.

## Changing host passphrases

We recommend that you change the administrative passwords from time to time. However, you will need administrator privileges to the host to do this. Create a

new password of at least 8 characters in length and use a mixture of character types.

To change the host passphrase

- 1 Connect to the host for which you want to change the passphrase.
- 2 Go to **Host > Change Host Passphrase**.  
The Passphrase Edit dialog box appears.
- 3 Enter the old host passphrase, the new passphrase, and the new passphrase for confirmation.  
The passphrase must be at least 8 characters in length and contain a mixture of character types.
- 4 Click **OK**.
- 5 Disconnect from the host.
- 6 Select **Host > Edit**.  
The Host Configuration dialog box appears.
- 7 Enter the new passphrase.
- 8 Click **OK**.  
You may now connect to the host. See [“Connecting to hosts”](#) on page 44.

## Connecting to the host using SSH

As a security feature, Symantec Decoy Server denies all remote connection attempts to the host. However, the administration console can give administrators permission to connect to the host using their own SSH client.

To SSH to the host

- 1 In the administration tree, select the icon of the host to which you want to SSH.
- 2 Click **Host > SSH**.  
The SSHd Daemon Start Complete dialog box appears and displays the SSH port number to which you can connect.
  - If you selected a Random SSH Port when adding or editing the host connection, this port number will be picked at random, therefore different each time.
  - If you specified an SSH Port number when adding or editing the host connection, you can connect using that port number each time.

- 3 Connect to the host IP address with the SSH port number using an SSH client.
- 4 Enter the login name and password you use for host access to complete this process.

---

**Note:** The Symantec Decoy Server sshd daemon will time out in one minute if a connection has not been established. It will then be necessary to repeat the previous steps.

---

## Editing host connections using SSH

If you want to edit the host connection parameters using SSH, you must also edit them in the Host Configuration dialog box. See [“Adding host connections”](#) on page 42.

To edit the host parameters

- 1 Disconnect from the host that you want to edit.  
See [“Disconnecting from hosts”](#) on page 47.
- 2 SSH to the host machine and edit the host connection parameters.  
See [“Host connection parameters”](#) on page 49.
- 3 Restart the host machine.
- 4 In the administration console, update the Host Configuration dialog box with the parameter changes.
- 5 Click OK.  
You may now connect to the host.

### Host connection parameters

The table below displays the locations of each parameter:

Table 4-3 Host Connection Parameters

Parameter Name	Location on the Host
Stealth Port	The port parameter listed under the “stealthd” heading in the <rti_home>/etc/qsp.conf file. Default: 12387

Table 4-3                      Host Connection Parameters

Parameter Name	Location on the Host
Username	<p>The &lt;username&gt; portion of the admin: &lt;username&gt;=&lt;passphrase&gt; parameter is listed in the &lt;rti_home&gt;/etc/passwd.conf file.</p> <p>Default: admin</p>
IP Address	<p>The host IP address is listed in the /etc/hosts file and the &lt;rti_home&gt;/etc/qsp.conf file. Both parameters must be edited if you change the IP address.</p> <p><b>Warning:</b> If you change the IP address, ensure that the host default router (etc/defaultrouter) and netmask (/etc/netmasks) is accurate.</p>
Administrative Network Device	<p>The device parameter is listed under the “stealthd” heading in the &lt;rti_home&gt;/etc/qsp.conf file.</p> <p>The device is supplied during the host installation.</p>

## Adding user accounts

Users are granted edit privileges based upon the group to which they are assigned; Operators, Administrators, and Managers. See “[User account privileges](#)” on page 51.

To enable other users to maintain, monitor, or administer the host and cages, the administrator must first add user account groups.

**Note:** Remember the group, user name, and passphrase you enter when adding user account. The user must provide this information in order to add the host to their local account.

To add a user account

- 1    Connect to the host with administrator permissions from your local administration console account.
- 2    Select **Host > Add User**.  
The Add User dialog box appears.
- 3    Enter a name in the User text box.

- 4 Select the Group access level you want to assign the user; Operator, Manager, or Administrator.  
See “[User account privileges](#)” on page 51.
- 5 Click **OK**.  
The Passphrase Edit dialog box appears.
- 6 Enter a unique passphrase for the user’s account. Re-enter the passphrase to confirm.  
The passphrase must be at least 8 characters in length and contain a mixture of character types.
- 7 Click **OK**.  
The Add User Confirm dialog box appears.
- 8 Click **OK**.  
You can now add the host connection to you local account.

## User account privileges

The table below shows the edit privileges granted to each user:

**Table 4-4** User Account Privileges

Privileges	Operator	Administrator	Manager
Host General Tab		X	X
Host Log Tab		X	X
Host Reports Tab		X	X
Cage Backup Tab		X	X
Cage General Tab		X	X
Cage Reports Tab	X	X	X
Cage Responses Tab	X	X	X
Log Viewer Queries	X	X	X
Restart Cages	X	X	X
Restart Host		X	X
Install Patches		X	X
SSH to Host	X*	X	X

Table 4-4            User Account Privileges

Privileges	Operator	Administrator	Manager
Change Host Passphrase	X	X	X
Add Users		X	X

\*While an operator can open a port for an ssh connection, they still require an account and password on the host for successful authentication.

## Uninstalling the Administration Console

To uninstall double click on the Uninstall icon in the Symantec Decoy Server folder or go to Add/Remove Programs in the Windows Control Panel and follow the instructions. Note that this will not remove the JRE, only the Symantec Decoy Server Administration console files.

# Activating product licenses

This chapter includes the following topics:

- [About the Symantec Enterprise Licensing System](#)
- [Activating a license](#)
- [Activating a license for upgrades](#)
- [Removing a License](#)

# About the Symantec Enterprise Licensing System

Symantec Decoy Server is activated by a license. Licenses are initially installed following product installation, through the Symantec Decoy Server Administration Console. When a license expires, a new license must be installed to renew the subscription.

---

**Warning:** If you are upgrading from an earlier version of Symantec Decoy Server, you will experience a break in functionality if you do not activate the license before installing the upgrade.

See [“Activating a license for upgrades”](#) on page 55.

---

## License warning and grace periods

When a license is within 30 days of the expiration date, it is considered to be in a warning period. You will receive alerts notifying you of the time to expiration. After a license expires, the licensed feature continues to operate for a grace period. You will receive alerts notifying you of how far past expiration your license is. If the grace period expires with no license renewal, all record of the license is removed and the product becomes unlicensed.

## Activating a license

To activate a license, you must have the serial number required for activation. The serial number is printed on the Symantec Serial Number Certificate for the product.

---

**Note:** The Symantec Serial Number Certificate is not part of the Symantec Decoy Server software distribution package, but is mailed separately and should arrive in the same time frame as your software.

---

### To activate a license

Activating a license is a two-step process.

- Obtain the license file from Symantec by completing the online form. You must have a serial number to complete the online form. Once you complete the online form, you receive the license file via email from Symantec.
- Install the license file that you receive via the Symantec Decoy Server Administration Console.

#### To obtain the license file

- 1 Open the Symantec Decoy Server Administration Console.
- 2 Connect to the host you wish to license.
- 3 On the menu bar, click **Host > Get Host ID**.
- 4 In the Host ID dialog box click **Copy Host ID to Clipboard**.
- 5 Open your web browser and point to <https://licensing.symantec.com/>.
- 6 Follow the instructions on Symantec's Licensing and Registration web page to complete the online licensing form.  
 You must have the appropriate serial number to complete the form.  
 The license file is returned via email as an attachment with the suffix .slf.  
 Make sure that the email address you provide on the online form is appropriate so that the license file will be accessible.

#### To install the license file

- 1 When you receive the email message from Symantec with the license file attachment, save the file to machine where you installed the Symantec Decoy Server Administration Console.
- 2 In the Symantec Decoy Server Administration Console click **Host > Install License**.
- 3 Select the appropriate Symantec license file.
- 4 When you are done installing the license file, your Symantec Decoy Server host will restart and you will have to reconnect.

## Activating a license for upgrades

If you are upgrading from an earlier version of Symantec Decoy Server and do not activate the license prior to installation you will experience loss of functionality. It is very important that you follow the procedure below if you are upgrading Symantec Decoy Server.

#### To activate a license for upgrade

- 1 Obtain a license file.  
 See [“To obtain the license file”](#) on page 55.
- 2 Copy the license file to your Symantec Decoy Server host machine.
- 3 Insert the Symantec Decoy Server CD in the host machine; mount the drive if necessary.

- 4 Change to the following directory:

```
# cd /cdrom/cdrom0/[platform name]/setup/bin
```

where [platform name] is the directory corresponding to the operating system installed on your SymantecDecoy Server host.

- 5 Get your Host ID by running `els_hit`.

```
# ./els_hit
```

- 6 Activate the license file on your host by running `els_lit`.

```
# ./els_lit [license file name]
```

## Removing a License

Symantec Decoy Server license files are not automatically uninstalled when the product is uninstalled. The license files remain in place, so that if you reinstall Symantec Decoy Server, the license is intact on reinstall. To remove an old Symantec Decoy Server license if you uninstall the product, you must delete two items by hand; the license directory on the host machine and the license file on the administration console machine.

---

**Note:** It is important to follow the process below if you uninstall Symantec Decoy Server, obtain a new license file, and reinstall it. If you do not, the reinstalled Symantec Decoy Server will not work.

---

To remove a license directory from the host

- 1 Log on to your Symantec Decoy Server host machine.
- 2 Remove the `/opt/Symantec/Licenses` directory.

```
# rm /opt/Symantec/Licenses/*.slf
```

After you have done this, you must delete the Symantec License File from the machine where you installed the Symantec Decoy Server Administration Console.

To remove the Symantec license file

- 1 On your administration console machine, change to the `<System Root>:\Program Files\Symantec\Decoy Server\` directory.
- 2 Remove any Symantec license files (\*.slf) you have installed in that directory.

# Setting Parameters

This chapter includes the following topics:

- [About setting parameters](#)
- [Editing parameters from the administration console](#)
- [Editing parameters from the command line](#)

## About setting parameters

Symantec Decoy Server uses parameter values to communicate with the host and cage, and to manage the log database. Many of these values are configured during the installation. You can modify parameters from the administration console or from the host command line.

## Editing parameters from the administration console

The following sections describe the parameters that you can modify from the administration console:

- [Editing host parameters](#)
- [Editing cage parameters](#)

Because some parameter values may be lengthy, it may be more convenient to copy and paste them from one host or cage to another instead of re-entering them from scratch. To copy, use the Copy item from the Edit menu, or select the word(s) you want to copy and press Ctrl-C. To paste, use the Paste item from the Edit menu, or press Ctrl-V. See [“Reverting host and cage parameters”](#) on page 62.

See [“Saving parameter changes”](#) on page 62 and [“Restarting hosts and cages”](#) on page 62.

### Editing host parameters

Symantec Decoy Server software uses host parameter values to construct a realistic environment within the cage, and specify how you to handle the log database.

To edit host parameters

- 1 Connect to the host.
- 2 Click the host tabs you want to edit.

See [“Host General tab”](#) on page 58 and [“Host Log Tab”](#) on page 59.

#### Host General tab

The host general parameters tab allow you to edit the home directory and specify the iButton (optional) device, as well as the commands the cages initialize upon startup.

To view host general parameters

- 1 Select a host from the administration tree and click the General tab.

---

**Note:** If you make changes to the host general parameters, you must save the changes and restart the host in order to effect the changes.

---

- 2 Edit the following parameters:

- **RTI Home Directory**—This parameter is not editable. This is the home directory of Symantec Decoy Server's file structure, <rti\_home>, created in the host installer.
- **iButton Device**—This specifies the communication port into which the iButton is plugged.

---

**Warning:** If you are using a SPARC machine for the host, do not plug the iButton into the primary (ttya) communication port, because Symantec Decoy Server will not function properly. See [“Installing a hardware token”](#) on page 20.

---

- **Default Cage Initialization Commands**—The value for this parameter specifies the default commands that each cage executes upon startup. The commands specified here are executed only if there are no initialization commands specified in the cage General tab. See [“Host General tab”](#) on page 58.

## Host Log Tab

The host log tab allows you to specify the failover log file location, the maximum log database size, and the IP address of the remote logging host.

To edit host log parameters

- Select a host from the administration tree and click the Log tab.
  - **Failover Log File Location**—The value for this parameter specifies the absolute path to the location to which Decoy Server will temporarily write the log files in the case of log database errors.
  - **Maximum Database Size**—The Maximum Database Size is used by the autocompressdb.sh script to specify the maximum size the log records in the log database can be before autocompressdb.sh compresses the current log records. Specify the Maximum Database Size in the number of megabytes. The default value is 100 MB.

---

**Note:** The `autocompressdb.sh` script is not scheduled to run by default, therefore the Maximum Database Size will not be used unless you configure `autocompressdb.sh`.

---

- **Remote Logging Host**—The value for this parameter is the IP address or host name of the remote host to which the flat file containing log records can be spooled. If this field is left blank, log files are kept on the host.

Symantec Decoy Server will identify the messages it sends to syslog as facility number 13 (log audit) and a priority based on the priority of the event logged. Syslog levels and their corresponding Symantec Decoy Server priorities are as follows:

Priority	Syslog Level	Description
128-256	crit	For warnings about critical conditions.
64-127	err	For other errors.
32-63	warning	For warning messages.
8-31	info	Informational messages.
0-7	debug	For messages that are normally used only when debugging a program.

The location on the remote syslog host to which the logs are written is specified by `syslog` in the `syslog.conf` file.

## Editing cage parameters

Cage parameters are initially specified at installation time, however, you may also edit cage parameters in the administration console.

To edit cage parameters

- 1 Connect to the host that houses the cage you want to edit
- 2 Click the cage icon in the administration tree.
- 3 Click the cage tabs you want to view or edit.

See [“Cage General tab”](#) on page 61 and [“Content Generation Module \(CGM\)”](#) on page 4.

## Cage General tab

The cage general parameters tab allows you to select a name for the cage, the actual cage network device, the decoy network device, and the cage startup commands.

To edit cage general parameters

- Select a cage from the administration tree and click the General tab.
  - **Hostname**—The value for this parameter is the actual cage hostname.
  - **Custom Name**—The value for this parameter is the name that you want to appear next to the cage icon in the administration tree.
  - **Default Route**—The value for this parameter is the name of the decoy network device that the intruder sees inside the cage.
  - **Actual Network Device**—The value for this parameter is the actual network device assigned to the cage.
  - **Decoy Network Device**—The value for this parameter is the name of the decoy network device that the intruder sees inside the cage.
  - **Initialization Commands**—The value for this parameter specifies the commands the cage executes upon startup. These commands override the Default Cage Initialization Commands specified in the host General tab. Enter the initialization commands in the following format, separated by a semi-colon:

```
command1;command2;command3
```

If you enabled Content Generation during the installation, the following commands will automatically appear in the Cage Initialization Commands:

```
/etc/rc2.d/S71rpc start  
/etc/rc2.d/S72inetsvc start  
/etc/rc2.d/S74syslog start  
/etc/rc2.d/S88sendmail start  
/etc/rc2.d/S88utmpd start;
```

- **Failover Log File Location**—The value for this parameter specifies the absolute path to the location to which Symantec Decoy Server will temporarily write the cage log files in the case of cage log database errors.
- **Content Generation Enabled**—This check box is enabled if you select Yes to content generation during the installation, otherwise it is greyed out. See [“Content Generation Module \(CGM\)”](#) on page 4.

## Saving parameter changes

You must save the changes you make in the administration console to the host and cage parameters. Save often to avoid losing any changes.

To save parameter changes

- For a host: select **Host** > **Save**.
- For a cage: select **Cage** > **Save**.

## Restarting hosts and cages

You can restart the hosts or cages from the administration console. You must restart the host to update the changes made to the host General and host Log tabs. You must restart the cage in order to effect changes made to the cage General tab.

To restart a host

- Select **Host** > **Restart**.

---

**Note:** This will take a few minutes.

---

To restart a cage

- Select **Cage** > **Restart**.

## Reverting host and cage parameters

You can undo any changes you made to system parameters at anytime before you save them.

To revert to the previously saved parameters of the selected host

- Select **Host** > **Revert**.

To revert to the previously saved parameters of the selected cage

- Select **Cage** > **Revert**.

## Editing parameters from the command line

You can edit parameters from the command line by using SSH to edit parameters in the `rti.conf` or `cage.conf` configuration files. See [“Command line parameters”](#) on page 63.

To edit parameters from the command line

- 1 SSH to the host machine. See [“Uninstalling the administration console”](#) on page 41.
- 2 Change to the <rti\_home>/etc directory.
- 3 Edit the host or cage parameters in the rti.conf or cage.conf files.
- 4 Save any changes to the files.
- 5 Restart the host machine.

## Command line parameters

The table below outlines the command line parameters for the rti.conf file.

Table 6-5 rti.conf parameters

rti.conf parameter name	Parameter name and location in administration console
RTIHOME	name: RTI Home Directory location: host General tab Note: Do not edit the RTIHOME parameter.
IBUTTONDEV	name: iButton Device location: host General tab
INIT	name: Default Cage Initialization Commands location: host General tab
LOGFILE	name: Failover Log File Location location: host Log tab
MAXLOGSIZE	name: Maximum Log Size location: host Log tab
LOGSERVER	name: Remote Logging Host location: host Logs tab

The table below outlines the command line parameters for the cage.conf file.

Table 6-6            cage.conf parameters

cage.conf parameter name	Parameter Name and Location in Administration Console
CAGENAME	name: Hostname location: cage General tab
CUSTOMNAME	name: Custom Name location: cage General tab
REALNETD	name: Actual Network Device location: cage General tab
FAKENETD	name: Decoy Network Device location: cage General tab
INIT	name: Initialization Commands location: cage General tab
LOGFILE	name: Failover Log File Location location: cage General tab
DEFAULTROUTE	name: Default Route location: cage General tab

# Configuring Response Policies

This chapter includes the following topics:

- [About configuring response policies](#)
- [Configuring response policies](#)
- [Understanding response filters](#)
- [Adding response filters](#)
- [Initiating a response](#)

## About configuring response policies

Response policies tell Symantec Decoy Server how to deal with the various types of host or cage activity, describing the actions that Symantec Decoy Server must take in response to events. This chapter describes response policy parameters and the process for configuring policies.

Understanding how events are related into event classes will help determine your response policies. For example, when a module detects a suspicious event, it relates the event to an event class and then Symantec Decoy Server can search for policies pertaining to the event class. You can also configure multiple responses for the same module or event class.

## Configuring response policies

The following sections describe the procedure for configuring response policies:

- [Adding response policies](#)
- [Selecting events](#)
- [Modifying response policies](#)

### Adding response policies

Adding response policies ensures that Symantec Decoy Server responds to an event, or a series of events, regardless of the severity of the compromise. See [“Configuring response policies”](#) on page 66.

To add a response policy

- 1 Select the icon of the host or cage in the administration tree.
- 2 Click the host or cage Response tab.
- 3 Click **Add Response**.  
The Response Policy Editor appears.
- 4 Select one of the following response types:
  - **SMTP**—Set the destination email address address, from email address address, and email subject.
  - **SNMP**—Supply the SNMP manager IP address and community string. Symantec Decoy Server sends SNMP v.1 traps and supports HP Openview, Tivoli, and Netcool.

- **ManHunt**—Supply the ManHunt IP address, the EDP port number (the default is 1333), the shared passphrase between Symantec ManHunt and Symantec Decoy Server, the IP address of the host or cage from which the events are sent and the vendor.

Symantec ManHunt response allows you to send Symantec Decoy Server events to a specified ManHunt node, enabling administrators to view both events from the ManHunt console. Symantec Decoy Server events are included in the activity to which ManHunt can respond, therefore, you can configure Symantec ManHunt policies on Symantec Decoy Server activity.

See the *Symantec ManHunt Installation Guide* for instructions on integrating with Symantec Decoy Server.

- **Custom**—Supply the name of the custom binary or shell script executable and the comma delimited arguments, if needed.  
Custom response allows you to launch your own application binaries or shell scripts in response to an event by specifying a command line which will be executed upon matching the policy.

---

**Note:** The custom response binary or shell script must be placed in the <rti\_home>/bin/alert directory and must be set to executable. In order for Symantec Decoy Server to execute a custom response, you must provide the name of the application binary or shell script as well as any arguments to pass on the command line (up to 255 characters long). The last argument specified in the Arguments parameter will be shown in the Data column of the log record.

---

Also, enter the following for each Response Type:

- **Response Interval**—Enter the frequency of the response in minutes. For example, if you set the interval to 5, you can expect a response approximately every 5 minutes as long as the event matches the specified policy. The first response will be sent as soon as the first match occurs.
- **Description**—Enter a description for the response policy. We recommend that you develop a naming convention to help you differentiate between the policies, such as naming the policies according to the specified event type or response type.

## 5 Click **Specify Policy**.

The Policy Events Editor appears.

## Selecting events

Symantec Decoy Server will respond to each event separately. Additionally, you may add a filter to a response policy once it is added. See [“Adding response policies”](#) on page 66.

To select host or cage events for response

- 1 Select the host or cage event(s) to which you want Symantec Decoy Server to respond.
- 2 Click **OK** in the Policy Events Editor and in the Response Policy Editor.
- 3 Select **Save** from the Host or Cage menu.

## Modifying response policies

You may modify response policies by following these steps. See [“Adding response policies”](#) on page 66.

To modify a response policy

- 1 Click on the response policy you want to modify in the response policy table. See [“Response policy characteristics”](#) on page 68.
  - If you are deleting policies, you can select multiple response policies by holding the Shift key while selecting the policies.
  - If you are editing a policy, you can also simply double-click the policy you want to edit.
- 2 Click **Edit Response**, **Duplicate Response**, or **Delete Responses**.  
If you are deleting policies, a verification dialog box appears that asks you to confirm that you want to delete the selected policies.
- 3 Click **Yes** to delete the policies.

## Response policy characteristics

The response policy table displays the following information:

- **Type**—The response type you selected, either SMTP, SNMP, Custom, or ManHunt.
- **Destination**—The response destination email address, SNMP string, executable, or ManHunt IP address.
- **Interval**—The response interval, specified in minutes, in which responses will be executed.

- **Description**—The description of the policy.

## Understanding response filters

The response filter tool provides a simple way to drop event types that you do not want Symantec Decoy Server to respond to.

The following sections describe Response filters:

- [Response filter format](#)
- [Response filter options](#)

The filters will vary, depending on the event type you are filtering, for example:

- For “Outgoing Connection,” you can filter based upon destination IP, destination port, and source IP.
- For “Stream Open Events,” you can filter based on stream ID and process ID.
- For “All Sensor Events,” you can only filter based upon priority and any arguments.
- “Response Type” actions are triggered if the event type matches all of the filters for an event, and none of the Exclude Filters.

### Response filter format

Depending on the event type you are filtering, you can enter integer filters, IP filters, or string filters.

Integer filters, such as Stream ID or Process ID, can only contain integers. IP address filters can contain integers, dots (.), and asterisks (\*) (to denote wild cards). For example, you can enter 10.10.\*.\* to filter all IP addresses from the 10.10 subnet. String filters can contain any valid regular expression.

You can choose between Including Filters and Excluding Filters. See [“Including filters”](#) on page 69 and [“Excluding filters”](#) on page 70.

### Including filters

Include Filters will allow Symantec Decoy Server to only respond when there is a match.

For example, if you want Symantec Decoy Server to respond when user “jjones” logs into the administration console, but not when any other user logs into the administration console, you can add a User Include Filter for the Administrative Logins response type.

## Excluding filters

Exclude Filters will narrow the activity to which Symantec Decoy Server responds.

For example, if you created a response policy for Symantec Decoy Server to respond for incoming connections, but you do not want to be alerted if it is an incoming connection from your IP address, 10.10.200.149, you can add an IP address Exclude Filter for the Incoming Connections response type.

## Response filter options

Options for each filter are described as either Host Filter Options or Cage Filter Options.

### Host filter options

The following are the possible host filter options:

- **iButton Module**—For all iButton Module activity, you can filter based upon any arguments.
- **Administrative Management Module**—For all Administrative Management Module activity, you can filter based upon the Source IP Address, User, or Any arguments.
- **Decoy Server Processes Module**—For all Symantec Decoy Server Processes Module activity, you can filter based upon Any arguments.

### Cage filter options

The following are the possible cage filter options:

- **Streams Module**—For all Streams Module activity, you can filter based upon the Stream ID, Process ID, Data, or Any arguments.
- **Process Module**—For all Process Module activity, you can filter based upon Command Arguments, the Process ID, Parent Process ID, User ID, Effective UID, Group ID, Effective GID, or Any arguments.
- **Filesystem Module**—For all Filesystem Module activity, you can filter based upon the File, Process ID, Major Number, Minor Number, or Any arguments.
- **Sniffer Module**—For all Sniffer Module activity, you can filter based upon the Destination IP Address, Source IP Address, Destination Port, Source Port, Data, or Any arguments.

## Adding response filters

You can add or modify the host or cage response policy to filter activity. See [“Modifying response policies”](#) on page 68.

To add response filters

- 1 Select **Add Response** from the Response tab.
- 2 Select **Specify Policy**.  
The Policy Events Editor dialog box appears. See [“Selecting events”](#) on page 68.
- 3 Right-click the event you want to filter.
- 4 Select **Edit Include Filter** or **Edit Exclude Filter** or **Frequency Filter** from the pop-up menu.  
The Include Filter or Exclude Filter or Frequency Filter dialog box appears.
- 5 If you are using the Frequency Filter, enter count and interval information as appropriate and click **OK**.
- 6 If you are using Edit Include Filter or Edit Exclude Filter, click **Add Filter**.  
The Filter Editor appears.

## Selecting response filters

After adding response filters, you may select a response filter. See [“Adding response filters”](#) on page 71.

To select a response filter

- 1 Select the type of filter you want to add from the Filter Type list.  
The arguments box under the Filter Type list changes according to the type of filter you select.
- 2 Enter arguments for the filter type in the arguments box.  
For example, if you want to exclude the user jjones from the User Login response, enter “jjones” in the Reg Ex Filter parameter.
- 3 Click **OK**.  
The filter policy will appear in the Include or Exclude Filters dialog box.
- 4 Click **OK** in the Include or Exclude Filters dialog box.

## Editing Response Filters

You can edit the host or cage response policy to filter activity. See [“Adding response filters”](#) on page 71.

To edit response filters

- 1 Select **Edit Response** from the Response tab.
- 2 Select **Specify Policy**.  
The Policy Events Editor dialog box appears.
- 3 Select **Edit Include Filter** or **Edit Exclude Filter** from the pop-up menu.  
The Include or Exclude Filters dialog box appears.
- 4 Click the response filter you want to edit or delete in the Include or Exclude Filters table,
  - If you are deleting filters, you can select multiple response filters by holding the Shift key while selecting the filters.
  - If you are editing a filter, you can also simply double-click the filter you want to edit.
- 5 Click **Edit Filter** or **Delete Selection**.  
If you are deleting filters, a verification dialog box appears that asks you to confirm that you want to delete the selected filters.
  - Click **Yes** to delete the filters.
- 6 Click **OK** in the Include or Exclude Filters dialog box.

## Initiating a response

To test if the Symantec Decoy Server SMTP, SNMP, or Symantec ManHunt responses are functioning properly, you can manually initiate a response. For SMTP responses, the script will output the session information between Symantec Decoy Server and the mail host.

To manually initiate a response

- 1 Change to the <rti\_home>/bin/alert directory.
- 2 Initiate one of the following responses:
  - To initiate an SMTP response, enter the following command:  

```
# ./smtp <to_address> <from_address> <subject> <message>  
<retry_interval>
```
  - To initiate an SNMP alert, enter the following command:

```
# ./snmp <dest_IP_address> <communityString> <message>
```

- To initiate a ManHunt response, enter the following command:

```
# ./mh-alert <edp receiver IP> <edp receiver PORT> <secret>  
<host/cage ip> <vendor> <message>
```

Where:

<edp IP> is the receiver IP.

<edp PORT> is the receiver PORT (enter 0 if not available).

<secret> must be fewer than 8 bytes in length.

<host/cage ip> is the IP address of the host/cage

<vendor> is a Symantec assigned vendor ID.

<message> Symantec Decoy Server log entry.

---

**Note:** Delimit each argument with a space. Within the argument, either delete spaces or enter an underscore to denote a separation between words. For example, for the <message> argument, enter “Decoy Server Alert!” as “Decoy Server\_Alert!”

Symantec Decoy Server will display if the response has been sent successfully and the session information between Symantec Decoy Server and the mail host.

---



# Creating Reports

This chapter includes the following topics:

- [About creating reports](#)
- [Selecting report types and parameters](#)
- [Generating reports](#)

## About creating reports

The reporting feature creates various types of reports based on host or cage log data. To use the reporting feature, you must provide values for report parameters, such as report start and end dates and data sorting and filtering parameters. The parameters you specify for a report are then saved as a “report policy” in the administration console for your convenience.

## Selecting report types and parameters

Reports are grouped by types and require that you supply various report parameters, depending on the type of report you are generating.

The following sections describe report types and their corresponding parameters:

- [General report options](#)
- [Scheduling options](#)
- [Date range options](#)
- [Data filter options](#)
- [Data display options](#)

### General report options

#### Report types

Reports types based on host or cage data are, by default, grouped by date. However, you may also group reports based on time. See “[Data breakdown options](#)” on page 80.

Aggregate groupings are useful when looking for attack patterns. For example, if you want to look for peak times when users attempt to access the cage. In this case, the report will display the number of attempted connections that occurred during the 1:00 A.M. hour, the 2:00 A.M. hour, and so on.

---

**Note:** Depending on the report type, you may also have the option of grouping the report type by category, such as IP address, port number, file name, or user name.

---

## Host report types

The Reports tab allows you to generate reports using the host report types described below.

- **Administrative Logins**—Reports the total number of administrative logins to the host by date. Administrative logins include connecting to the host from the administration console, as well as successful logins to the host machine. If a date was not listed, then there were no successful logins on that date.
  - **Administrative Logins Aggregate**—Reports the total number of administrative logins to the host by aggregate time.
  - **Administrative Logins By User**—Reports the total number of administrative logins to the host by user.
- **Admin Logouts**—Reports the total number of administrative logouts from the host by date. Administrative logouts include disconnecting from the host from the administration console, as well as successful logouts from the host machine. If a date was not listed, then there were no successful logouts on that date.
  - **Admin Logouts Aggregate**—Reports the total number of administrative logouts from the host by aggregate time.
- **Custom Report**—Reports the results of the user's custom query, grouped by the day, week, and month that the events occurred.
  - **Custom Report Aggregate**—Reports the results of the user's custom query results by the hour, day, week, and month that the events occurred.
  - **Custom Report By Field**—Reports the query results by the field the user chooses.

## Cage report types

The Reports tab allows you to generate reports using the cage report types described below.

- **File Modifications**—Reports the names of the files that were opened for writing by an intruder by date. If a date during the time interval was not listed, then there were no files opened for writing on that date.
  - **File Modifications Aggregate**—Reports the names of the files that were opened for writing by an intruder by aggregate time.
  - **File Modifications By File**—Reports the names of the files that were opened for writing by file.

- **Log Entries**—Reports the number of log records recorded by date, records a log entry and assigns a priority number for any cage activity. See also Appendix A “Event Types”. See also “Event Types”. If a date during the time interval was not listed, then no log records were recorded on that date.
  - **Log Entries Aggregate**—Reports the number of log records recorded by aggregate time.
  - **Log Entries By Priority**—Reports the number of log records recorded by priority number.
- **Overall Cage Summary**—Reports the number of responses triggered, outgoing connections, UDP port activity, attempted connections, and file modifications that occurred during the defined time interval.
- **Responses Triggered**—Reports the number of responses triggered by date. The number of responses generated depends on the policies configured in the cage Responses tab. See also “Adding Response Filters” on page 6-8. See also Adding Response Filters.

If you configured SNMP and SMTP response policies, both specified to alert on Outgoing Connections, the report will list two alerts triggered for outgoing connections on that date, one for each policy. If a date during the time interval was not listed, then no responses were triggered on that date.

  - **Responses Triggered Aggregate**—Reports the number of responses triggered by aggregate time.
  - **Responses Triggered By Priority**—Reports the number of responses triggered by priority number.
- **Successful Logins**—Reports the number of times a user successfully accessed the cage by date. A successful login can indicate a possible attack, for example if an intruder overflows the buffer and gains shell access. A user can also successfully log into the cage with a correct user name and password. If a date was not listed, then there were no successful logins on that date.
  - **Successful Logins Aggregate**—Reports the number of times a user successfully accessed the cage by aggregate time.
- **Attempted Connections**—Reports the number of attempted TCP connections made to the cage by date. Examples of attempted connections are port scans, telnet requests, and HTTP requests.
  - **Attempted Connections Aggregate**—Reports the number of attempted TCP connections made to the cage by aggregate time.
  - **Attempted Connections By IP**—Reports the number of attempted TCP connections made to the cage by source IP address.

- **Outgoing Connections**—Reports the number of outbound TCP/IP connections from the cage by date. An intruder might initiate an outgoing connection if, for example, they successfully log into the cage and FTP to a home machine to upload a rootkit. If a date was not listed, then there were no outgoing connections on that date.
  - **Outgoing Connections Aggregate**—Reports the number of outbound TCP/IP connections from the cage by aggregate time.
  - **Outgoing Connections By IP**—Reports the number of outbound TCP/IP connections from the cage by destination IP address.
- **TCP Port Activity**—Reports the port activity generated by attempted TCP connections to the cage by date. For example, if an intruder telnets to a cage, Symantec Decoy Server logs a connection attempt to port 23 for TCP Port Activity. If a date was not listed, then there was no TCP port activity on that date.
  - **TCP Port Activity Aggregate**—Reports the port activity generated by attempted TCP connections to the cage by aggregate time.
  - **TCP Port Activity By Port**—Reports the port activity generated by attempted TCP connections to the cage by port number.
- **UDP Port Activity**—Reports the port activity generated by attempted UDP connections to the cage by date. For example, if an intruder launches a UDP port scan at the cage, Symantec Decoy Server logs a connection attempt to the port specified during the scan for UDP Port Activity. If a date was not listed, then there was no UDP port activity on that date.
  - **UDP Port Activity Aggregate**—Reports the port activity generated by attempted UDP connections to the cage by aggregate time.
  - **UDP Port Activity By Port**—Reports the port activity generated by attempted UDP connections to the cage by port number.
- **Port Activity**—Reports the port activity generated by attempted TCP and UDP connections to the cage by date. If a date was not listed, then there was no port activity on that date.
  - **Port Activity Aggregate**—Reports the port activity generated by attempted TCP and UDP connections to the cage by aggregate time.
  - **Port Activity By Port**—Reports the port activity generated by attempted TCP and UDP connections to the cage by port number.
- **Custom Report**—Reports the results of the user's custom query, grouped by the day, week, and month that the events occurred.

- **Custom Report Aggregate**—Reports the results of the user's custom query results by the hour, day, week, and month that the events occurred.
- **Custom Report By Field**—Reports the query results by the field the user chooses.

## Data breakdown options

The data breakdown options that are available depend on the report type you select. The options are also interpreted differently depending on the report type.

- **Data Breakdown Options for Reports by Date**—If you select a report type that groups data by date, then you can further break down the data by day, week or month.
  - **Day**—The report will display the number of events per calendar day during the time period you specify. For example, if you select Log Entries, Symantec Decoy Server will display the number of log entries for December 1, 2001, December 2, 2001, and so on. If a day is not listed in the report then no events were detected during that day.
  - **Week**—The report will display the number of events per week during the time period you specify. Symantec Decoy Server displays the week by number, with 52 total weeks per year. For example, Week 1, 2002 corresponds to the first week of January, 2002. If a week is not listed in the report then no events were detected during that day.
  - **Month**—The report will display the number of events per month during the time period you specify. For example, if you select Log Entries, Symantec Decoy Server will display the number of log entries for December 2001, January 2002, February 2002, and so on. If a month is not listed in the report then no events were detected during that month.
- **Data Breakdown Options for Reports by Aggregate Time**—If you select a report type that groups data by aggregate time, you can break down the data by hour, day, week or month.
  - **Hour**—The report will display the aggregate number of events per hour during the time period you specify. There are 24 possible hours in a day, and Symantec Decoy Server aggregates the events from all corresponding hours. For example, the report displays the total number of events that occurred during the 14th hour, or 2 P.M. of all days within the time period.
  - **Day**—The report will display the aggregate number of events per day during the time period you specify. There are 31 possible days in a month, and Symantec Decoy Server aggregates the events from all

corresponding days. For example, the report displays the total number of events that occurred on the 1st of all months within the time period.

- **Week**—The report will display the aggregate number of events per week during the time period you specify. There are 52 weeks in a year, and Symantec Decoy Server aggregates the events from all corresponding weeks within the time period. For example, if the report period spans three years, Symantec Decoy Server determines the number of events that occurred during Week 1 of each year, adds them up, and displays the total number of events that occurred during Week 1 of all three years together.
- **Month**—The report will display the aggregate number of events per month during the time period you specify. There are 12 months in a year, and Symantec Decoy Server aggregates the events from all corresponding months within the time period. For example, if the report period spans three years, Symantec Decoy Server determines the number of events that occurred during January of each year, adds them up, and displays the total number of events that occurred during January of all three years together.
- **Data Breakdown Options for Reports by Category**—If you select a report that groups data by a specific category, such as port or IP address, the data breakdown option will not be available.

## Results sort order

The results for all report types can be displayed in ascending or descending order.

For example, if you selected a report By Date and an Ascending sort order, the report will display the earliest date first and the most recent date last.

## Report name

This is the name you choose for your report.

## Scheduling options

Scheduling options apply only to scheduled reports.

- **Schedule this Report**—Click the check box if you wish to schedule this report for future viewing.
- **Destination**—Enter an email address to which the reports will be sent.
- **From**—Enter the email address from which the reports will be sent.

- **Interval (in days)**—Enter the interval, in days, at which the reports will be sent.
- **Send Next Report At**—Enter the date and time at which the next report will be sent. Specify the time in Military Time, from 00 to 23 hours. The succeeding reports will be sent on the hour and on the interval you specified.

## Date range options

The Date Range options allow you to specify an absolute or relative date range as described below, or you can select Include All Dates for each report.

### Absolute date range

You can enter absolute start and end dates to specify a fixed time range.

For example, if you want a report summarizing the activity that occurred from January 1, 2002 to January 15, 2002, you can enter January 1, 2002 as an absolute start date and January 15, 2002 as an absolute end date.

### Relative date range

You can enter start and end dates relative to the time you configure the report policy. Relative dates are useful if you want a report summarizing the activity that occurred during the past day, week, or month.

For example, to generate daily reports summarizing only the day's activity, enter a start date as 1 day relative to now and an end date 0 days relative to now. To summarize the week's activity, enter a relative start date of 7 and a relative end date of 0.

## Data filter options

To instruct Symantec Decoy Server to completely disregard particular data from reports or only include particular data in reports, you can use the Include or Exclude Filter List in the Data Filter Options dialog box. This feature provides a simple way for you to drop event types you do not want to see in the reports. You can include a filter when adding or editing report policies.

For example, if you select a report type that groups the data by port number, such as TCP Port Activity By Port, you will be able to include or exclude data based on the port number but not by IP address.

In addition to the default, user, port, priority, etc. filters provided, the user can now specify a filter on any valid field.

For example, if you're generating a port activity report, and you want to exclude all records from host 1.2.3.4, you can simply add: [ip-src]1.2.3.4; to the exclude port filter text field. You can also exclude ports, like 30-120;

The generic format of the advanced filter is: [<qsp field>]<actual filter>

The following sections describe filter options, depending on the report type you select:

- [Port filter](#)
- [Priority filter](#)
- [File filter](#)
- [IP address filter](#)
- [User filter](#)
- [Number of results to display](#)

## Port filter

The port filter is available to all report types with report names ending in By Port, such as the TCP Port Activity By Port report. You can exclude or include reported data on activity occurring on specific ports by entering the port numbers in this parameter.

For example, if you do not want to view the number of times HTTP requests were made to the cage in the Total TCP Port Activity report, you can enter 80 in the Exclude Port Filter parameter.

Conversely, if you only want to view the number of times HTTP requests were made to the cage in the Total TCP Port Activity report, you can enter 80 in the Include Port Filter parameter. Separate each port number by a semicolon. Port filters can include ranges.

For example, the following Exclude Port Filter entry will exclude port 10 and all ports between 20 and 180:

```
10;20-180
```

## Priority filter

The priority filter is available to all report types with report names ending in By Priority, such as the Log Entries By Priority report. You can exclude or include specific priority numbers from the reports by entering the priority numbers in this parameter.

For example, if you do not want to include entries of priority 64 [Suspicious] in the Log Entries By Priority report, you can enter 64 in the Exclude Priority Filter parameter.

Conversely, if you only want to include entries of priority 64 [Suspicious] in the Log Entries By Priority report, you can enter 64 in the Include Priority Filter parameter. Separate each priority number by a semicolon. Priority filters can include ranges.

For example, the following Exclude Priority Filter will exclude all priority numbers between 32 and 63:

```
32-63
```

## File filter

The file filter is available to all report types with report names ending in By File, such as the File Modifications By File report. You can exclude or include specific ports from the reports by entering the absolute paths to the files in this parameter.

For example, if you do not want to view the number of times the /dev/null file was modified in the File Modifications report, you can enter /dev/null in the Exclude File Filter parameter.

Conversely, if you only want to view the number of times the /dev/null file was modified in the File Modifications report, you can enter /dev/null in the Include File Filter parameter. Separate each file path by a semicolon. File filters can be exact or substring matches.

For example, the following Exclude File Filter will exclude the file /etc/hosts as well as all files whose paths contain bin:

```
î/etc/hostsî;bin
```

## IP address filter

The IP address filter is available to all report types with report names ending in By IP, such as the Outgoing Connections By IP report. You can exclude or include specific IP addresses from the reports by entering the IP addresses in this parameter.

For example, if you do not want to view the number of times your home machine, IP address 10.10.200.57, accessed the cage in the Total Attempted Connections report, you can enter 10.10.200.57 in the Exclude IP Address Filter parameter.

Conversely, if you only want to view the number of times your home machine, IP address 10.10.200.57, accessed the cage in the Total Attempted Connections

report, you can enter 10.10.200.57 in the Include IP Address Filter parameter. Separate each IP address by a semicolon. IP address filters can contain an asterisk “\*” to denote a wild card.

For example, the following Exclude IP Address filter will exclude all IP addresses of the 10.0.1 class as well as the IP address 12.12.12.12:

```
10.0.1.*;12.12.12.12
```

## User filter

The user filter is available to all report types with report names ending in By User, such as the Admin Logins By User report. You can exclude or include specific users from the reports by entering the user names in this parameter.

For example, if you do not want to view the number of times “jjones” connected to the host from the administration console in the Admin Logins By User report, you can enter “jjones” in the Exclude User Filter parameter.

Conversely, if you only want to view the number of times “jjones” connected to the host from the administration console in the Admin Logins By User report, you can enter “jjones” in the Include User Filter parameter. Separate each user name by a semicolon. User filters can be exact or substring matches.

For example, the following Exclude User Filter will exclude the user admin as well as all users whose names contain jones:

```
!admin!;jones
```

## Number of results to display

You can limit the number of results to display in the report by specifying an integer in the Number of Results to Display parameter.

For example, if you select the Admin Logins report type, select the Descending results sort order, and enter a value of 100 for the Number of Results to Display parameter, the report will list the earliest 100 logins.

## Data display options

The data display options available depend on the report type you select.

- **Select Chart Type**—Enabled if you are creating a Report policy; scheduled reports are only sent in text format. The options are pie chart, table, column chart, line chart, or text file. The format you select determines the format that the report dialog box will first display the report. However, the report dialog box allows you to subsequently view the report data in any of these formats.

- **Resolve IP Addresses**—Enabled if you are adding a policy for a report type that reports IP addresses, such as the Attempted Connection By IP report. Select this option to resolve IP addresses within the report to their domain names.
- **Include Data from All Cages**—Enabled if you are creating a policy for a cage report. Select this option if you want the report to include relevant data from all cages on the host. Do not select this option if you want to view data for only the selected cage.

## Custom query editing options

If you add a custom query report type, you are also given custom query editing options.

- **Group Data by\Filter On**—Allows you to enter a count on any field that you select for a custom report.
- **Query Name**—Displays the name as Custom Report Query.
- **Match ANY of these terms**—Allows you to define a query term that will return a match on ANY of the term parameters except Time.
- **And All of these terms**—Allows you to define a query term that will return a match on ALL of the term parameters except Time.

## Generating reports

You can generate reports automatically from the administration console. Symantec Decoy Server generates reports in a pie, column, line, table and text view. Depending on the report type, you can also save reports as TXT, HTML, PNG or PDF files.

To generate reports

- 1 Select the Reports tab and click on the report you want to generate.
- 2 Click **Generate**.

The Report Generation dialog box appears.

---

**Note:** Allow a few seconds for the full report data to load when you generate a report.

---

- 3 Click the **Show Generated Reports** check box to view the report immediately, or click the **Save Reports to HTML** to save the report.

- 4 Click OK.
  - If you choose to show a generated report the Report Views dialog box appears with tabs for pie, column, line, table and text view options. See [“To display report options”](#) on page 87.
  - If you choose to save a report, the Save generated HTML to . . . dialog box appears and allows you to browse and locate a folder where you would like to save the HTML files.

## Displaying report options

When choosing to show a generated report, the Report Views dialog box appears with tabs for pie, column, line, table and text view options. See [“Generating reports”](#) on page 86.

To display report options

- 1 Select a view from the Pie, Column, Line, Table or Text tab in the Report Views dialog box.
- 2 Click **Display All Records** to show all the records used to generate the report.
  - Click the **Strip Control Characters** check box to remove the control characters before displaying the query results.
  - Click the **Resolve IP Addresses** check box if you want the query results to include the domain names that correspond to the IP addresses in the results.
- 3 Click **Save** if you would like to save the report.  
Reports including:
  - Tables can be saved as HTML or PNG files.
  - Charts can be saved as PNG or PDF files.
  - Text can be saved as TXT or PDF files.
- 4 Click **Print** to generate copy of the report if desired.
- 5 Click **Close** when you are finished viewing the report.

## Generating reports though the log viewer

You can generate reports based on the options in the log viewer dialog box by selecting this option on the Reports tab for the host or cage. When you generate a report through the log viewer the option to schedule a report is excluded. This corresponds to the idea that log viewer reports are simple graphical

representations of the results queried, and are, therefore, based only on the minimum options need to create a report.

To generate a report from the log viewer

- 1 Select the Report tab for the host or cage and click **View Host Log** or **View Cage Log**.  
The Log Viewer dialog box for the host or cage appears.
- 2 Select the time frame for the report.
- 3 Choose a query in the Select Query drop down box.
  - Click the **Strip Control Characters** check box to remove the control characters before displaying the query results.
  - Click the **Resolve IP Addresses** check box if you want the query results to include the domain names that correspond to the IP addresses in the results.
- 4 Click **Apply**.
- 5 Click **Yes** to run the query as live or **No** to not run the query as live.

To view details of any event reported

- 1 Double-click on any event.
- 2 Click **Help** for information on event types and possible responses.

To save a report generated from the log viewer

- 1 Click **File > Generate Report on Data . . .**
- 2 Select an action from the action drop-down box.
  - **Generate**—allows you to view report data as a pie, column, line, table and text view on the fly.
  - **Generate and Save**—allows you to view report data and save it under the Report tab.
  - **Save**—allows you to save report data under the Report tab for viewing later.

For the remaining generate report data options, see [“Selecting report types and parameters”](#) on page 76.

# Managing Cage Sessions

This chapter includes the following topics:

- [About managing cage sessions](#)
- [Getting started](#)
- [Running cage sessions](#)
- [Creating a custom cage](#)
- [Creating a legal disclaimer banner](#)

## About managing cage sessions

Cages are virtual environments on the host that an intruder can explore and change.

To conduct a cage session you must install customized content in the cage for interaction. Before you access the cage, you must add a cage user account, and set the user and cage root passwords. See [“Getting started”](#) on page 90.

## Getting started

To prepare the cage for a session follow these steps:

- [Adding a cage user account](#)
- [Setting the user password](#)
- [Setting the cage root password](#)

When you are finished, you can install customized content in the cage for interaction by establishing a pseudo terminal PTY (pseudo teletype) session with the cage. See [“Establishing a cage session”](#) on page 92.

## Adding a cage user account

A standard UNIX security feature is that you cannot gain root access to a host through a remote connection. Therefore, if you want to telnet into the cage, you first have to login as a normal user. To do so, you must add a cage user and then set the password for that user. See [“Setting the user password”](#) on page 90 and See [“Setting the cage root password”](#) on page 91.

To add a user for cage access

- 1 SSH to the host. See [“Connecting to the host using SSH”](#) on page 48.
- 2 Change to the <rti\_home>/bin directory.
  - If, for example, you want to add a user account and home directory for jjones, run the following script:

```
# ./rti.useradd <cage#> -m -d i/export/home/jjonesi jjones
```

## Setting the user password

If you have added a cage user account, you may continue by setting the user password. See [“Adding a cage user account”](#) on page 90.

To set the user password

- 1 From the `<rti_home>/bin` directory, run the following script to set the password for the new user, `jjones`:  

```
# ./rti.passwd <cage#> jjones
```
- 2 When prompted, enter a password for `jjones` that will be saved in the `passwd` file.

## Setting the cage root password

After setting the user password, you may set the cage root password. See [“Setting the user password”](#) on page 90.

Now that you can log in as the user, you may escalate to the superuser by specifying the correct root password. The root accounts within the cages are disabled upon install, therefore you must set the root password.

To set the cage root password

- 1 SSH to the host. See [“Connecting to the host using SSH”](#) on page 48.
- 2 Change to the `<rti_home>/bin` directory.
  - If, for example, you want to use the default `<rti_home>` directory, `/usr/decoy` use the following command:  

```
# cd /usr/decoy/bin
```
- 3 Run the following script so that you can set the root password:  

```
# ./rti.passwd <cage#> root
```
- 4 When prompted, enter a root password to gain superuser access within the cage.

## Running cage sessions

A cage session allows you to install applications, and create a false set of data files and user directories for a cage. See [“Creating a custom cage”](#) on page 97.

The following sections describe how to run cage sessions:

- [Establishing a cage session](#)
- [Editing cage IP addresses](#)
- [Editing CGM user accounts](#)
- [Modifying cages bypassing the log](#)

- [Starting and stopping cages](#)
- [Backing up cages](#)
- [Restoring cages](#)

## Establishing a cage session

After you have added a cage user and set the cage root password, you can establish a cage session. See [“Getting started”](#) on page 90.

To establish a cage session

- 1 Telnet into the cage as the cage user, for example, jjones.
- 2 Enter the user password when prompted.
- 3 Become the superuser by entering the su command at the prompt.
- 4 Enter the cage root password.

You can now interact with, and/or make changes to the cage.

## Editing cage IP addresses

If, for any reason, you need to change the cage IP addresses, the steps below will allow you to do this.

To edit the cage IP addresses

- 1 SSH to the host. See [“Connecting to the host using SSH”](#) on page 48.
- 2 Edit the /etc/hosts file.
  - If, for example, you want to use the vi text editor, run the following command:  

```
# vi /etc/hosts
```
- 3 Edit the cage IP address.
- 4 Restart the host machine.

---

**Note:** It may take a few minutes for the host and cages to load.

---

## Editing CGM user accounts

If you enabled the Content Generation Module (CGM) during the host installation, as your organization’s employee information changes, you may want

to add, edit, or delete CGM user accounts. You can add accounts with specified information or generate random accounts.

To create user accounts in a cage

- 1 Log on to your Symantec Decoy Server host machine.
- 2 Change to the following directory:

```
# cd /decoy/bin/
```

- 3 If you want to create a specific user account, run `rti.makeuser`:

```
# ./rti.makeuser <cageNum> <acct_name> <gender> <realname>
```

<code>cageNum</code>	Which cage to modify (1-4).
<code>acct_name</code>	The account name you wish to create within the cage, e.g., <code>jsmith</code> .
<code>gender</code>	The gender of the user (0 for female, 1 for male).
<code>realname</code>	The name, in quotes, of the user you wish to create within the cage, e.g. <code>Jane Smith</code> .

This will add your custom user to the new user file.

---

**Note:** The roster file keeps track of all the cage users that the CGM knows about. The new user file is a roster of employees waiting to be added to the roster file. They will be added to the roster file the next time `rti.usergen` is run.

---

- 4 To generate random users and update the roster file with your custom users run `rti.usergen`:

```
# ./rti.usergen <cageNum> <key> <nrand> <rerun> <make-mail>
```

<code>&lt;cageNum&gt;</code>	Which cage to modify (1-4).
<code>&lt;key&gt;</code>	A random number.
<code>&lt;nrand&gt;</code>	The number of randomly generated users to add to the cage. If you only wish to add a specified user to the cage, set this to 0.

<code>&lt;rerun&gt;</code>	<ul style="list-style-type: none"> <li>■ If <code>rerun = 0</code>, <code>rti.usergen</code> uses the users on the host as the base set of users. It removes all users in the cage's <code>/etc/passwd</code>, <code>/etc/shadow</code>, and <code>/cgm/content/addrs</code> files. It will not, however, remove home directories for users previously generated on the cage.</li> <li>■ If <code>rerun = 1</code>, <code>rti.usergen</code> will add new users to the cage without deleting old ones.</li> </ul>
<code>&lt;make-mail&gt;</code>	Whether or not to generate email for the users in the roster file (0 = no, 1 = yes).

- 5 Log on to the Administration Console.
- 6 Connect to your host by clicking on it in the left hand pane and selecting **Host > Connect** from the menu bar.
- 7 Restart your cage by selecting **Cage > Restart** from the menu bar.

---

**Note:** New users will not be added until you restart your cage. If you add users within the cage using `useradd`, they will not appear when the cage is restarted.

---

#### To delete user accounts from a cage

- 1 Log on to your Symantec Decoy Server host machine.
- 2 Change to the following directory:

```
# cd /decoy/bin/
```

- 3 Run `rti.deluser`:

```
# ./rti.deluser <cageNum> <acct_name>
```

`cageNum` Which cage to modify (1-4).

`acct_name` The account name you wish to delete within the cage, e.g., `jsmith`.

You may wish to view the current user accounts in a cage.

#### To view current user accounts in a cage

- 1 Log on to your Symantec Decoy Server host machine.
- 2 Change to the following directory:

```
# cd /decoy/bin/
```

### 3 Run `rti.listusers`:

```
# ./rti.listusers <cageNum>
```

`cageNum` Which cage to view (1-4).

You may wish to view the user accounts waiting to be added to the roster file.

To view new user accounts in a cage

#### 1 Log on to your Symantec Decoy Server host machine.

#### 2 Change to the following directory:

```
# cd /decoy/bin/
```

### 3 Run `rti.newusers`:

```
# ./rti.listusers <cageNum>
```

`cageNum` Which cage to view (1-4).

## Modifying cages bypassing the log

If you want to execute commands in the cage without logging them, you may use the `rti.cagedo` command. This allows you to perform operations as if you were in the cage but with all of the capabilities of the host. Symantec Decoy Server utilities `rti.useradd`, `rti.passwd` and `rti.userdel` use `rti.cagedo` to execute Solaris commands, `useradd`, `passwd`, and `userdel` in the context of the cage.

If, for example, you want to install software through `pkgadd` and put the package into the filesystem, log in as root to the host:

```
<RTIHOME>/cage#/root/...(wherever)
```

then, execute:

```
<RTIHOME>/bin/rti.cagedo <RTIHOME>/cage#/root pkgadd ...
```

This will install the package in the cage as if logged into the cage as root, with the notable exception that nothing will be logged.

## Starting and stopping cages

You can start, stop, and restart individual cages from the administration console or from the host command line. You may want to stop a cage, for example, if you suspect that an intruder is doing a large amount of damage to the cage. The cages will automatically load when the host starts.

To start, stop, or restart a cage from the administration console

- 1 Select the icon of the cage you want to start, stop, or restart from the administration tree,
- 2 Select either **Start**, **Stop**, or **Restart** from the Cage menu.

---

**Note:** It may take a few seconds for the cages to stop.

---

To start or stop a cage from the host command line

- 1 SSH to the host. See [“Connecting to the host using SSH”](#) on page 48.
- 2 Change to the <rti\_home>/bin directory.
- 3 Run the following script to start or stop a cage:

```
# ./cagemanctl [start|stop] cage <cage#>
```

- If, for example, you want to stop cage 2, enter the following:

```
# ./cagemanctl stop cage 2
```

## Backing up cages

During the installation, you were given the option to create a backup copy of the cage to later restore the cage if it becomes damaged. If you selected “Yes”, you can update the backup file with any subsequent changes made to the cage, such as any installed content or modifications made to the cage parameters.

If the cage has been damaged, you can then restore the cage back to its original condition. The new backup copy overwrites the existing cage backup file. You can also update or restore cages from the host command line.

To backup the cage from the administration console

- 1 Select the icon of the cage you want to backup from the administration tree.
- 2 Select the Backup tab and click on the Backup Enabled check box.
- 3 Enter the directory path for the backup location of your cage.
- 4 Select **Cage > Stop**.
- 5 Select **Cage > Backup**.
- 6 Select **Cage > Start**.

To backup the cage from the command line

- 1 SSH to the host. See [“Connecting to the host using SSH”](#) on page 48.

- 2 Change to the <rti\_home>/bin directory.
- 3 Run the following backup or restore a cage:  

```
# ./cagemanctl backup <cage#>
```

  - If, for example, you want to update the cage 2 backup file, enter the following command:  

```
# ./cagemanctl backup 2
```

## Restoring cages

If a cage becomes damaged for any reason, you can use the cage backup file to restore the cage. See [“Backing up cages”](#) on page 96.

To restore a cage from the administration console

- 1 Select the icon of the cage you want to restore from the administration tree.
- 2 Select **Cage > Stop**.
- 3 Select **Cage > Restore**.
- 4 Select **Cage > Start**.

To restore a cage from the command line

- 1 SSH to the host. See [“Connecting to the host using SSH”](#) on page 48.
- 2 Change to the <rti\_home>/bin directory.
- 3 Run the following backup or restore a cage:  

```
# ./cagemanctl reload <cage#>
```

  - If, for example, you want to update the cage 2 backup file, enter the following:  

```
# ./cagemanctl backup 2
```
  - If you want to restore cage 2, enter the following:  

```
# ./cagemanctl reload 2
```

## Creating a custom cage

You can customize your cage to make it resemble one of your organization's application servers. Although the customization options are endless, this administration guide includes tips on creating a custom Web Server, FTP Server and Database Server. To maximize the effectiveness of each Symantec Decoy Server server on the network, ensure that customized cage contents are

sufficiently realistic so as to engage the attacker as long as possible. The longer an attacker remains inside a cage, the more data the logs will be able to collect.

To install customized content into the cage

- 1 Add a cage user account. See [“Adding a cage user account”](#) on page 90.
- 2 Set the user password. See [“Setting the user password”](#) on page 90.
- 3 Add a root password. See [“Setting the cage root password”](#) on page 91.
- 4 Establish a session with the cage. See [“Establishing a cage session”](#) on page 92.
- 5 Install customized content in the cage. See [“Creating a custom cage”](#) on page 97.

---

**Warning:** Only install custom content within the cage if you disabled the Content Generation Module (CGM) during the host installation. If the CGM is enabled within the cage, all of your customization will be overwritten.

Also, if you install applications outside the cage, do not bind the application to a port currently being used by an application within a cage. Binding a port both inside and outside the cage causes network instability.

---

## Web server

This section describes the steps necessary to create custom cages for various types of servers.

If the computer being protected by Symantec Decoy Server is the Web server for the public Web site, it is best to mirror the public Web site files into the cage because intruders expect them to be there. These files may even be the intruders' target if their purpose is to vandalize your Web pages. You can allow the attacker to work for you by discovering weaknesses in the CGI scripts, javascript and other code used on your site.

Before beginning the customization process for a Web server decoy, obtain the following:

- Installation media for the Web server.
- Access to copies of the actual Web site files, for example HTML, ASP, and CGI files, sanitized if necessary.
- Installation media for other cages in the cluster if a decoy cluster will be created.
- Hardware for each Symantec Decoy Server server in the cluster

To properly imitate the Web server, place a copy of the Web site in the cage. If the site is extensive, it may not be necessary to copy the entire site to the cage. However, the Web site files and directories should be updated whenever the actual site changes and it may be simpler to copy the entire site into the cage than to select only certain portions for copying.

## FTP server

Before beginning the customization process for an FTP server decoy, obtain the following:

- FTP server installation media
- Content for the FTP decoy server

The content for an FTP decoy does not need to be sanitized if the content is publicly accessible. If the content is provided for a fee, it may be wise to sanitize it. For example, if the decoy is for a software retail site. Key files required to run the software can be removed so that the attacker remains connected long enough to download the files, but will not discover the uselessness of the files until later.

If the content is confidential to the company, the content should be sanitized, but file names should retain an authentic look.

Content should be updated as often as the real FTP server content is updated. If decoy content is not updated periodically, the decoy content becomes less and less interesting to an attacker as the files age.

## Database server

Before beginning the customization process for a database server decoy, obtain the following:

- Installation media for the database
- Sanitized content

The decoy content should resemble the types of data in the database server being protected. A decoy human resources server can be an especially attractive target with its potential for revealing sensitive data about employees, benefits and salaries. For example, set up tables with columns for employee names, addresses, and other data kept by the company on its employees. The amount of data should accurately reflect the size of the company. The frequency with which a database server decoy should be updated depends on how often the actual server is updated.

## Creating a legal disclaimer banner

To protect the company legally, it is recommended that you post a disclaimer banner in each cage.

To create a legal disclaimer banner

- 1 Create an issue file and place it in the `<rti_home>/cage<#>/root/etc` directory.  
The issue file is automatically displayed before the user logs in, if not
- 2 Edit the `motd` (message of the day) file in the `<rti_home>/cage<#>/root/etc` directory.  
The message of the day is automatically displayed after the user logs in.
- 3 Place the legal disclaimer banner in the file you created.

### Example of a legal disclaimer banner

Remember to alter this example so that it does not enable attackers to identify the machine as a cage.

#### NOTICE TO USERS

Use of this system constitutes consent to security monitoring and testing. By using this system, the user consents to any interception, monitoring, recording, copying, auditing, inspection or disclosure at the discretion of authorized site or corporate personnel.

Unauthorized or improper use of this system may result in administrative disciplinary action and civil and criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this warning.

# Managing the Log Database

This chapter includes the following topics:

- [About managing the log database](#)
- [Creating queries](#)
- [Querying log records](#)
- [Replaying sessions](#)
- [Verifying log records](#)
- [Rotating and compressing log records](#)
- [Restoring logs](#)

## About managing the log database

The log database collects data about intruders inside of cages, such as the source Internet Protocol address and port number to track the attack source.

The log database can also be used to view host and cage events in real-time. Although host and cage logs are written to the same log database, they are viewed from separate log viewers.

From the log viewer, records can be queried, sorted, compressed and printed. You can also replay cage PTY (pseudo teletype) sessions to view an intruder's interaction with the cage. See ["Replaying sessions"](#) on page 112.

Additionally, event logs are signed by the iButton to verify their authenticity. See ["iButton"](#) on page 5.

## Creating queries

To begin, you must query the log for the events you want to view. Symantec Decoy Server provides several predefined queries that search the logs for common host and cage events. You can also configure your own custom log database queries.

The following sections describe the various types of queries:

- [Adding predefined queries](#)
- [Adding custom queries](#)

### Adding predefined queries

Predefined queries allow you to search for events that occur on host and cage log data. The log viewer displays matching records for any single predefined query. You can also launch multiple log viewer dialog boxes and view the results of a succession of predefined queries.

See the sections below for details:

- [Host log data](#)
- [Cage log data](#)

#### Host log data

- **All Records**—Displays all host log records.
- **Admin Logins**—Displays all successful logins to the administration console.

- **Admin Sessions**—Displays all successful activity through the stealth service, including administration console logins, servers starting (either the qsp proxy for communicating to the logs or sshd) and servers stopping. This query allows you to see the beginning and the end of all valid administration console sessions.
- **Invalid Connection Attempts**—Displays all invalid traffic sent to the stealth service. This includes incorrect logins to the administration console, invalid traffic sent to the stealth service, and replay attempts (an intruder attempting to use the ID of a captured session to gain access).
- **iButton Records**—Displays any messages from the iButton, such as signature or verification errors, or expiration warnings.
- **Errors and Warnings**—Displays all errors and warnings logged from the Symantec Decoy Server modules.

## Cage log data

- **All Records**—Displays all cage log records.
- **PTY Session Activity**—Displays all activity that occurred during an established PTY (pseudo teletype) session with a cage. For example, if an intruder successfully telnets to a cage, all keystrokes entered and output to the screen are recorded as PTY Session Activity.
- **File System Activity**—Displays the names of all files opened for writing.
- **Invoked Processes**—Displays all processes that have been executed within the cage.
- **Network Activity**—Displays all incoming UDP or TCP connections, as well as connection attempts. Incoming connections include telnet connections, FTP connections, and port scans. These log records will contain the source and destination IP addresses and ports.

## Adding custom queries

Custom queries allow you to search terms by specifying three term parameters—the Key, the Value for the Key and the Operator as described below:

- **Key**—The type of data you want to query for, such as the source IP address or user ID.
- **Operator**—Specifies how the query will determine whether a particular log entry matches the query.
- **Value**—The specific value for the Key.

For example, if you select the Source IP Key, enter a Value of 10.0.1.166, and select the = Operator, the query will return only those log entries that contain the IP address 10.0.1.166.

You can also define a query term that will return a match on ANY or ALL of the term parameters except Time. You must also enter either a String or an Integer argument, depending on the type of Key you select. An argument is made up of the Value you enter and the Operator you select. See [“Operators”](#) on page 105 and [“Query search parameters”](#) on page 109.

To add custom queries

- 1 Click the **View Host Log** or **View Cage Log** button in the lower right corner of the administration console.  
The Log Viewer dialog box appears.
- 2 Select **Query > Add**.  
The Custom Query Edit dialog box appears.

## Selecting query search parameters

After adding a custom query, you may select query search parameters. See [“Adding custom queries”](#) on page 103.

To query for each term exclusively

- 1 Enter a name for the query.
- 2 Click **Add** under the Match ANY of These Terms box.  
The Term Editor dialog box appears.

To query for a combination of terms inclusively

- 1 Enter a name for the query.
- 2 Click **Add** under the or Match ALL of These Terms box.  
The Term Editor dialog box appears.

## Selecting query search values

After selection query search parameters, you may select query search values. See [“Selecting query search parameters”](#) on page 104.

To select query search values

- 1 From the Key list, select the activity you want to query. See [“Query search parameters”](#) on page 109.

- 2 Select an operator and enter a value.

---

**Note:** You cannot enter a value for Event or Module. Instead, select from the drop list of values.

---

- 3 Repeat the previous steps for each term you want to add to the query.

- 4 Click **Save**.

The query name is added to the Select Query drop-down list in the Log Viewer dialog box. See [“Selecting columns”](#) on page 111.

## Operators

The following table describes the operators you can assign:

Table 10-7 Operators

Operators:	Module	IP	String	Integer	Description
=	X	X	X	X	The query results will include only those log entries that contain the exact Key value you specified.
<=				X	The query results will only include those log entries if they contain Key values less than or equal to the Key value you specified. For example, if you want to query for all events of a Critical (128-256) priority, you can select the “Priority” key, select the “<=” operator, and enter the integer “256”.
<				X	The query results will only include log entries if they contain Key values that are less than the value you specified.
>				X	The query results will only include log entries if they contain Key values greater than the value you specified.
>=				X	The query results will only include log entries if they contain Key values greater than or equal to the value you specified.
!=	X	X	X	X	The query results will only include log entries if they do not contain the Key values you specified.

Table 10-7 Operators

Operators:	Module	IP	String	Integer	Description
~=		X	X		<p>The query results for the “pattern match operator” vary, depending on the data in the field to be matched. For text fields, like description and data, the ~= operator matches as a POSIX regular expression. For example, searching for description ~= “^ERROR.*” would match any description beginning with ‘ERROR’. When applied to IP addresses the ~= operator will match the network instead of host addresses. Specify the network address in one of two ways:</p> <p>ip-src ~= 10.0.1.* -or-</p> <p>ip-src ~= 10.0.1.0/24</p> <p>(Both of these match any address on the 10.0.1.0 - 10.0.1.255 network.)</p> <p>The ~= operator is not applicable to number fields like cage number and time, which use the &gt; and &lt; operators.</p>

Duplicating custom queries

You can duplicate any custom query, including the predefined queries.

To duplicate custom queries

- 1

In the Log Viewer, click the Select Query drop-down list, select the custom query that you want to duplicate.
- 2

Select **Query > Duplicate**.  
A new entry for the duplicate will be listed in the Select Query drop-down list.

Editing and deleting custom queries

You can edit or delete any custom query you add. However, you can not edit or delete a predefined query.

To edit or delete custom queries

- 1

In the Log Viewer, click the Select Query drop-down list, select the custom query that you want to edit or remove.
- 2

Select **Query > Edit** or **Query > Delete**.
  - If you select Delete, a confirmation dialog box appears in which you click **Yes** or **No** and the process is complete.

- If you select **Edit**, the Custom Query dialog box appears.
- 3 Under the **Match ANY of These Terms** or **Match ALL of These Terms** boxes, select the term you want to edit and click **Edit**.  
The Term Editor dialog box appears.
- 4 Edit the term and click **OK**.
- 5 Repeat the previous two steps for each term you want to edit.
- 6 Click **Save** in the Custom Query dialog box to save your changes.

## Querying log records

To run a predefined or custom query, you must enter the start and end dates. The query will only return event data that occurred within the date range you specify.

There are also two options you can select:

- **Strip Control Characters**—Check this option if you want to remove the control characters before displaying the query results.
- **Resolve IP Addresses**—Check this option if you want the query results to include the domain names that correspond to the IP addresses in the results.

To query the log records

- 1 In the administration tree, click the icon of the host or cage for which you want to view log data.
- 2 Click **View Host Log** or **View Cage Log** in the lower right corner of the console.  
The Log Viewer dialog box appears.
- 3 Enter the start and end dates.  
The query will only return event data that occurred within the date range you specify.
  - For the end date, you can check the **Now** box to view the logs until the current time.
- 4 Select a predefined or custom query from the **Select Query** drop-down list.
- 5 Click **Strip Control Characters** if you want to remove the control characters from the log records.
- 6 Click **Resolve IP Addresses** to display the IP addresses with their corresponding domain names.
- 7 Click **Apply**.

- If you selected Now for the end time, the Live Update dialog box appears.
- 8 Click **Yes** to view the log records in real-time.  
The matching log records appear in the Log Viewer table. See [“Selecting columns”](#) on page 111 and [“Sorting query results”](#) on page 111.

---

**Note:** When viewing the logs, if you get a “-207 Results Truncated” error, the number of records searched was larger than the SearchLimit value and no log records will be displayed. See [“Search limit”](#) on page 108.

The administration console refuses to display a possibly invalid result set. To view the log records, refine the query so that the log viewer returns fewer results.

---

## Search limit

By default, the log database will query a maximum of 10,000 records in order to maintain optimal performance. If the query you perform requires more than 10,000 records to be searched, an error will appear indicating that records have been truncated from the search. These records, however, remain in the log database. To avoid truncating records from the results, refine the query or decrease the date range you are querying. You can disable or change the value of the search limit parameter by editing the qsp.conf file.

To change the log database search limit

- 1 SSH to the host. See [“Editing host connections using SSH”](#) on page 49.
- 2 Change to the Symantec Decoy Server etc directory, for example:  

```
# cd /usr/decoy/etc
```
- 3 Open the qsp.conf file with a text editor such as vi.  

```
# vi qsp.conf
```
- 4 Edit the value assigned to the SearchLimit, which is by default 10000.
  - Assign a value of 0 if you do not want a search limit.
- 5 Save changes to the qsp.conf file.
- 6 Restart the host machine.

## Query search parameters

The data returned by a query is sorted and displayed in the columns described in the table below. The columns are displayed even if the query returned no data for a particular column. See [“Selecting columns”](#) on page 111.

The information displayed depends on the module that detected the event. See [“Selecting report types and parameters”](#) on page 76.

**Table 10-8** Query search parameters

Parameter	Description
Arguments	The arguments, if any, that were entered by the intruder. The rti.proclog module reports this column.
Data	The data that triggered the event detection. The rti.stealthd, rti.sniffd, and rti.strlog modules report this column.
Description	A brief description of the event. All modules report this column.
Destination IP	The cage IP address to which the intruder attempted to connect. The rti.sniffd module reports this column.
Destination Port	The service to which the intruder attempted to connect. The rti.sniffd module reports this column.
Effective GID	The effective group identifier, which is the GID to which the group escalated. The rti.filesys, rti.procf, and rti.proclog modules report this column.
Effective UID	The effective user identifier, which is the UID to which the user escalated. The rti.filesys, rti.procf, and rti.proclog modules report this column.
Event	The name assigned to the event. See also Appendix A Event Types. All modules report this column.
File	The file that was accessed by the intruder. The rti.filelog module reports this column.
Group ID	The intruder's group identifier (GID) of the process. The group identifiers are located in the etc/groups file. The rti.filesys, rti.procf, and rti.proclog modules report this column.
Device Major	The major device number associated with the device that was accessed. The rti.filelog module reports this column.
Decoy Server User	The name of the user that logged in to the administration console. The rti.stealthd module reports this column.

Table 10-8      Query search parameters

Parameter	Description
Device Minor	The minor device number associated with the device that was accessed. The rti.filelog module reports this column.
Module	The module that detected the event. All modules report this column.
Parent PID	The process ID that forked a child process. The rti.proclog module reports this column.
Priority	The priority number Symantec Decoy Server assigned to the event. All modules report this column. See also “Event Priority” on page 9-13.
Process ID	The unique process ID assigned to the session. The rti.filesys, rti.procfs, rti.strlog, and rti.proclog modules report this column.
Source IP	The source IP of the intruder. The rti.stealthd and rti.sniffd modules report this column.
Source Port	The service assigned to the incoming connection. The rti.sniffd module reports this column.
Stream ID	The unique ID assigned to an opened PTY session. The rti.strlog module reports this column.
User ID	The intruder's user identifier (UID) of the process. The user identifiers are located in the etc/passwd file. The rti.filesys, rti.procfs, and rti.proclog modules report this column.

## Event priority

Symantec Decoy Server assigns each event both a priority number between 0 and 256 and a category, either Information, Important, Suspicious, or Critical. The following are the event priority ranges:

Table 10-9 Event Priority

Priority	Category	Event Types
0-31	Informational	Information events notify administrators of operational logging under normal circumstances.
32-63	Important	Important events should be noted, but they do not necessarily indicate a cage security compromise.
64-127	Suspicious	Suspicious events should be investigated further. Possible security compromises are labeled as Suspicious events. Examples of suspicious events include when the host detects a packet, when keystrokes are recorded within a cage, when any user executes a process, or when someone port scans the host or attempts to log in to a cage.
128-256	Critical	Critical events should be responded to immediately. Critical cage security compromises are labeled as Critical events. Examples of critical events include when an attacker breaks into a cage and sends a packet to the network, creates a new pseudo terminal such as FTP or telnet, or runs a process as root.

## Selecting columns

The Log Viewer dialog box displays the results of your selected query. All queries do not necessarily display data in all columns, so you may want to remove the empty columns from the display, or you may only want to view certain types of data returned by the query.

To select the columns you want to view

- 1 Click **Edit > Select Columns**.  
The Select Columns dialog box appears.
- 2 Select the columns you want to view and click **OK**.

## Sorting query results

You can sort log records either alphabetically or numerically.

To sort log query results

- 1 Click the heading of the column you want to sort.
- 2 Shift-click the column heading to reverse the sorting order.

## Printing query results

Symantec Decoy Server allows you to print the query results displayed in the Log Viewer. Only the displayed columns will be printed.

To print the log records

- 1 Run a log query. See [“Querying log records”](#) on page 107.
- 2 Select the columns you want to print. See [“Selecting columns”](#) on page 111.
- 3 Select **File > Print**.

## Exporting query results

You can export the log records you are viewing into a CSV (Comma Delimited ASCII) spreadsheet compatible with Microsoft Excel™ or any other spreadsheet or database.

To export the log records

- 1 Run a log query. See [“Querying log records”](#) on page 107.
- 2 Select **File > Export**.
- 3 Browse for a directory to which to save the log records and enter a name for the log data file.
- 4 Click **Save**.

# Replaying sessions

Each time an intruder logs into a cage using applications such as telnet, ssh, or rlogin, Symantec Decoy Server records the keystrokes the intruder entered, as well as the output written to the screen. These PTY (pseudo teletype) sessions can be replayed at any time in the administration console. You can choose the session, labeled by the initial time and date of the established session, and the speed the session will be replayed. Session Replay also allows you to view live sessions, enabling you to see in the intruder’s actions in real-time.

To replay a cage session

- 1 Open the Log Viewer for the cage by selecting **View Cage Log** from the bottom right corner of the Administration dialog box or **View Log** from the Cage menu.
- 2 Select **Database > Session Replay**.  
The Terminal Session Monitor dialog box appears.

## Selecting a PTY session

After you have selected to replay a cage session, you can select a PTY session.

To select a PTY session

- 1 Select a session from the panel by clicking it.  
The sessions are labeled by the date and time the intruder first logged into the cage.

---

**Note:** If you see a date followed by “live”, an intruder is currently inside the cage. The “live” status will disappear once the intruder quits the session.

---

- 2 Click **Play**.
  - Click the local echo check box if you would like the local echo switch to echo intruder’s keystrokes in the replay window and in the user input window. Local echo is useful for seeing things that don’t normally echo back, like passwords, but otherwise produces double characters.
  - If you do not click the local echo check box, the User screen panel displays output written to the intruder’s screen, while the User input panel displays intruder’s keystrokes for the session.
- 3 Adjust the playback control speed in the upper left-hand corner of the dialog box, if necessary.
- 4 To clear the User screen panel click **Reset**. The session you are replaying will continue to play in a clear panel.

You can also replay a session by viewing the PTY Session Activity log records and double-clicking a record that is within the session you want to view.

See [“Querying log records”](#) on page 107.

## Verifying log records

You may need to use log records as evidence at some point. To be useful as evidence, the log files should meet the requirements described below. Even if you

do not anticipate the need to use logs as evidence, it is advisable to maintain your records according to these standards to create a history of normal usage that can be compared with any abnormal activity logged on the server.

- Logs must be preserved unedited. The administration console gives you the option of spooling the logs to a remote host.
- The logs must contain entries for all superuser activities, all user logins and logouts, all use of resources, and email traffic data.
- Logs must be maintained consistently over time; presenting a couple of days or weeks worth of logs may not be sufficient to establish a history of normal usage.

To verify the log records from the administration console

- In the host or cage Log Viewer, select **File > Verify Log**.  
A message appears in the progress meter indicating whether the verification was completed or if it failed.

---

**Note:** Backups of all logs should be kept.

---

## Log verification failure

If the log database fails to verify the log records, the following are possible causes:

- Someone has compromised the host and altered the log database records.
- The log database has been shutdown and restarted while log records were being written. Records are signed in blocks. Therefore, if the log database is halted in the middle of a block, the affected block will not be signed by the iButton.
- The log database file has been corrupted.

## Possible solutions

Perform the solutions in the order listed below

- 1 Compress the log database to force the log database to create a new block.  
This will ensure that future log records are properly signed by the soft token or iButton.
- 2 Look for other irregularities that might lead to a root cause of the problem.
- 3 Visit the Symantec Support at <http://support.symantec.com/>.

# Rotating and compressing log records

To enable faster database performance, Symantec Decoy Server allows you to tune the database. When a log record is older than a defined time, in seconds, the record will either be deleted or moved from the primary database to the backup database. For example, you can delete records that are over 15 days (1,296,000 seconds) old, or you can move records that are over 15 days old from the primary log database to the backup database.

For optimal performance, we recommend that you trim or compress the logs in the primary log database when the primary database is holding approximately 100,000 log records. The time it takes for the log database to reach 100,000 records will vary, depending on the amount of activity the host and cage experiences. See [“Verifying total log records”](#) on page 115.

---

**Note:** When users wish to retrieve ALL records at once, the database should not be allowed to grow more than approximately 10,000 records or whatever the value of SearchLimit parameter is in /etc/qsp.conf.

---

The following sections describe the various ways to tune the log database:

- [Verifying total log records](#)
- [Trimming log records](#)
- [Manually compressing log records](#)
- [Automatically compressing log records](#)

## Verifying total log records

You can verify the total number of records in the log database to help you determine how many records you need to safely trim for optimal performance.

Symantec recommends that you trim or compress the logs in the primary log database when the primary database is holding approximately 100,000 log records. See [“Trimming log records”](#) on page 116.

To verify the total records in the log database

- 1 Select a host or cage and click on the **View Host Log** or **View Cage Log** button.
- 2 Click **Database > Total Records**.
- 3 Click **OK**.

## Trimming log records

You can configure Symantec Decoy Server to automatically trim old log records from the primary log database for faster performance. Old logs can be deleted or moved to the backup log database. Backup log records can be restored so that you can view them in the Log Viewer. See [“Restoring backup logs”](#) on page 118.

To trim old log records from the primary log database

- 1 SSH into the host. See [“Editing host connections using SSH”](#) on page 49.

- 2 Change to the `<rti_home>/etc` directory.

The following example uses the Symantec Decoy Server default directory:

```
# cd /usr/decoy/etc
```

- 3 Open the `qsp.conf` file with a text editor such as `vi`.

```
# vi qsp.conf
```

- To delete the expired log records, edit the event parameter under the [Flags] heading as follows:

```
event = sant
```

-or-

- To move the expired log records to the backup database, edit the event parameter under the [Flags] heading as follows:

```
event = santb
```

- 4 Under the [DB] section of the `qsp.conf` file, edit the `MaxRecordAge` parameter so that its value is equal to the age in seconds at which the records can be trimmed. For example, if you want all records over 10 days old to be trimmed, set:

```
MaxRecordAge = 864000
```

where 864,000 is the number of seconds in 10 days.

---

**Note:** If you set a value for the event parameter but do not set a value for the `MaxRecordAge` parameter, then the `MaxRecordAge` defaults to a value of 0, indicating that records should never be trimmed.

---

- 5 Save the changes made to the `qsp.conf` file.
- 6 Restart the host machine with the “init 6” command.

## Manually compressing log records

You can manually compress all host and cage log records currently in the primary and backup log database. When you compress the log database, records from both the primary and backup log database will be compressed. You can not compress the backup logs separately. See [“Automatically compressing log records”](#) on page 117.

To manually compress logs

- Open the host or cage Log Viewer, and select **File > Compress**.

The compressed log database files will be located in the `<rti_home>/db/backup` directory and named `db-YYYYMMDDHHMMSS.tar.bz2`, where `YYYYMMDDHHMMSS` is the date and time at which the log was compressed. See [“Restoring compressed logs”](#) on page 119.

## Automatically compressing log records

To configure Symantec Decoy Server to automatically compress the logs, you must create a scheduled (cron) job to run the `autocompressdb.sh` script. The script will test the size of the logging database, and if it is larger than the defined Maximum Database Size it will compress the current log records. See [“Restoring compressed logs”](#) on page 119.

---

**Note:** When the `autocompressdb.sh` script is run, Symantec Decoy Server will compress all host and cage log records currently in the primary and backup log database, making the log records unavailable for querying.

---

To automatically compress the logs

- 1 In the administration tree, select the icon of the host whose log database you want to compress.
- 2 Set the Maximum Database Size in the Host Log tab. Specify the value for this parameter in number of kilobytes. The default value is 100,000 KB. The following steps describe how to add a cron job to run the `autocompressdb.sh` script.
- 3 SSH to the host. See [“Editing host connections using SSH”](#) on page 49.
- 4 Change to the `/var/spool/cron/crontabs` directory.  

```
# cd /var/spool/cron/crontabs
```
- 5 Edit the root crontab.

```
# crontab -e
```

- 6 Add the following line to the crontab file to run the autocompressdb.sh script every night at midnight:

```
00 00 * * * <rti_home>/db/autocompressdb.sh
```

where <rti\_home> is the home directory, by default /usr/decoy.

When autocompressdb.sh runs, it will compress the database files if they are larger than the Maximum Database Size.

## Restoring logs

You can restore log records to the primary database that have been moved to the backup database, or that have been automatically or manually compressed.

The following sections describe the how to restore logs:

- [Restoring backup logs](#)
- [Restoring compressed logs](#)

### Restoring backup logs

Before you restore the backup logs, the log database must be stopped. This results in the temporary inaccessibility of the current records. Any new data is appended once the backup logs are restored to the Log Viewer.

---

**Warning:** We strongly recommend that you stop your cages before restoring the backup log records.

---

To restore backup logs to the primary log database

- 1 Disable log trimming.
- 2 Open the <rti\_home>/etc/qsp.conf file with a text editor such as vi.  
The following example uses the <rti\_home> default directory, /usr/decoy:

```
# vi /usr/decoy/etc/qsp.conf
```

- 3 Under the [Flags] heading, change event=satb to event=sa.
- 4 Save changes to the qsp.conf file.
- 5 Stop the log database.

```
# /usr/decoy/bin/logdb.sh stop
```

- 6 Change to the <rti\_home>/db directory, which is by default /usr/decoy/db.

**7** Enter the following commands:

```
mv ./db-files/event.dat ./db-files/event.old
mv ./db-files/event.bak ./db-files/event.dat
```

**8** Restart the log database.

```
# <rti_home>/bin/logdb.sh start
```

The backup logs will be restored to the primary log database and can be viewed in the Log Viewer.

**9** To send the records to the backup database, replace the mv commands in step 4. with the following:

```
mv ./db-files/event.dat ./db-files/event.bak
mv ./db-files/event.old ./db-files/event.dat
```

## Restoring compressed logs

To view log records that have been compressed either automatically or manually, you must restore the records back to the primary log database. However, restoring the records will overwrite any existing records in the log database without warning. Before restoring compressed log records, we recommend that you manually compress the current log records.

---

**Warning:** We strongly recommend that you stop your cages before restoring the compressed log records.

---

To restore compressed logs to the log database

**1** Change to the db directory, which is by default /usr/decoy/db.

**2** Enter the following command:

```
# ./uncompressdb.sh backup/<compressed_log>
```

Compressed logs are labeled db-YYYYMMDDHHMMSS.tar.bz2, where YYYYMMDDHHMMSS is the date and time at which the log was compressed.



# Responding to Attacks

This chapter includes the following topics:

- [Determining IP ownership](#)
- [Taking legal action](#)

## About responding to attacks

Symantec Decoy Server puts you in control of responses to attempted security breaches on your network by detecting and collecting data on all types of attacks, known and unknown. Whereas, traditional intrusion detection systems will not recognize new attacks because they are looking for known attack signatures. For example, MapTrap log data helps you determine the IP address of the intruder.

With the data you collect from Symantec Decoy Server, you get to decide whether to simply prevent the intruder from making future attacks based on data you gathered, or to actually use the data to apprehend the intruder with the help of authorities.

## Determining IP ownership

If you want to contact the administrator for the system through which your network has been attacked, you must first identify the owner of the IP address, and then obtain the contact information for that system's administrator. The IP address for the attacking system appears in the log file.

---

**Note:** In the log files, be sure to not mistake 127.0.0.1 for the address of the attacking system. Any machine will try to connect to itself if you try to connect to 127.0.0.1. This address appears in the log files because the log messages are being received from the local machine.

---

Use the `whois` command to retrieve the system administrator contact information from Internet registries such as ARIN.NET, the American Registry for Internet Numbers, as in the following example:

```
# whois -h whois.arin.net 204.189.52.2
```

This command example returns the following response:

```
Cable & Wireless USA (NETBLK-CW-02-BLK) CW-02-BLK 204.188.0.0 -  
204.189.255.255  
  
BEST INTERNET (NETBLK-CW-204-189-0A) CW-204-189-0A 204.189.0.0 -  
204.189.63.255
```

For more information about one record, enter `whois !` followed by the handle shown in parentheses following the name. To determine the point of contact for Best Internet in the example above, you would enter the following command:

```
# whois !NETBLK-CW-204-189-0A
```

In `csh`, `tcsh` and similar shells that treat the `!` as a special character, you may have to escape the `!` with a backslash character. For example:

```
# whois \!NETBLK-CW-204-189-0A
```

You may have to use additional whois commands depending on the response you receive to the first whois command. For example, responsibility for the address may have been assigned to another party. After you have obtained the contact information, you can then contact the administrator about the incident.

Alternatively, you can use the ARIN whois database search page at <http://www.arin.net/whois> to look up numeric IP address owners.

## Taking legal action

If your organization intends to prosecute an attacker, the most important legal issue is the actual cost of recovery and not the amount of lost revenue. In the US, the cost of activities related to the cost of recovery should be carefully documented. For example, the number of hours spent by particular departments to restore machine configurations or data, find and remove any back doors or Trojan horses left behind by the attacker, and so on. See information on cybercrime legislation. Also, consult your state and local authorities regarding state and local legislation that may affect your ability to prosecute a particular offense.

In order for the data collected in the logs to be admissible as evidence, the attacker must be presented with a legal disclaimer upon being sent to the Symantec Decoy Server machine. See “[Creating a legal disclaimer banner](#)” on page 100.

Because disclaimers are commonly posted on servers, the appearance of such a banner on the Symantec Decoy Server machine will not distinguish it from other servers on the network. It is best to post legal disclaimers on all machines on your network to inform users that they can not depend on their data or activities being confidential. If employees are not informed of this fact and forced to acknowledge it each time they log in to the network, you may face legal difficulties when attempting to retrieve data from the network that the employee believed to be private.



# Troubleshooting

This chapter includes the following topics:

- [Configuration checker](#)
- [Installation errors and solutions](#)
- [Administration console errors and solutions](#)
- [Alerting errors and solutions](#)
- [iButton errors and solutions](#)
- [Testing an iButton](#)
- [Cage failure](#)
- [Reporting problems](#)

## Configuration checker

The configuration checker is a utility that checks the setup for many common configuration problems.

To run the CheckConfig script

- 1 SSH to the host. See [“Editing host connections using SSH”](#) on page 49.
- 2 Execute `<rti_home>/bin/CheckConfig`.  
The script will analyze the configuration and describe any possible problems it finds.
  - Issues preceded by an asterisk (\*) may be automatically fixed by executing the generated script called `/rtihome/bin/fixme`.
  - Remaining issues should be manually fixed after running CheckConfig and fixme.

## Installation errors and solutions

The following are some common errors you may experience during the host installation:

- [Host verification](#)
- [Cannot access floppy drive](#)
- [System crash during restart](#)
- [Wrong OS](#)
- [Lack of permissions](#)
- [Problem accessing the certificate](#)
- [iButton installation problems](#)
- [Lack of disk space](#)
- [Insufficient resources](#)

### Host verification

After you have installed the host and administration console, verify that the installation has been done correctly.

To verify the host installation:

- Ping the machine.
- If you cannot ping the machine, check the network hardware and verify that the cage has the appropriate network settings.

## Cannot access floppy drive

You are unable to access the floppy disk which is in the drive. The `volcheck -v` command returns “no media was found”; however, the floppy media is in the drive. Ensure that the volume manager daemon (`vold`) is running. You can issue the command, “`ps -ef | grep vold`” to check. If it is not running, you can start it by issuing the following command:

```
/etc/init.d/volmgt start
```

## System crash during restart

If the system panics and crashes during restart, determine if OS patches were installed after the cages were created. If so, the entire Symantec Decoy Server system must be re-installed.

---

**Note:** OS patches cannot be installed into an existing system.

---

## Wrong OS

Be sure that the tar ball you are using is for your specific host machine. If you are installing on Solaris, run the command `uname -a` to be sure the machine is running SPARC Solaris 7 or 8 with full distribution and OEM support.

## Lack of permissions

You must have write permissions to the install location to look at interfaces. It is best to run the installer as a root capable user. The customer may want you to run as a separate `UID=0` user to track you separately.

## Problem accessing the certificate

To access a certificate

- 1 Make sure the diskette is mounted.
- 2 Run the `df` command to see which filesystems are mounted.

- On Solaris, enter `ps -ef | grep vold` to ensure that the volume manager daemon (vold) is running.  
If vold is not running, you can start it by entering `/etc/init.d/volmgt start`.
- 3 Run the `volcheck -v` command.
- 4 Double-check the path to the floppy to ensure that it is entered correctly.

## iButton installation problems

The iButton may have been damaged in transit, tampered with, or may just have a bad connector. If the following errors appear during the installation, refer to the corresponding solution below:

Table 12-10 iButton errors and solutions

Error	Solution
f100	The iButton is experiencing problems. See <a href="#">“Testing an iButton”</a> on page 133.
f200	Can not find the iButton. Ensure that the iButton is securely placed inside the caddy.
f300	Can not find the iButton caddy. Ensure that the iButton caddy is properly attached to the appropriate communication port.
f400	Can not communicate with the iButton. Ensure that the proper serial port is selected, typically <code>/dev/ttyb</code> .

## Lack of disk space

The installation requires a minimum of 2 gigs free disk space for the host plus 2 gigs for each cage. Use the `df -k` command to ensure that the partition you are installing in has enough disk space.

## Insufficient resources

There may be insufficient disk space, memory, or CPU. Check disk space with the `df -k` command. There must be a minimum of 2 gigs per cage plus 2 gigs for the host software in the partition in which you install Symantec Decoy Server. For example, if you install four 2-gig cages, allocate a minimum of 10 gigs in a single partition. If you configure the mount points for a cage larger than 2 gigs, for

instance a 4-gig file server, you must allocate a minimum of 4 gigs for that cage. Allow space for applications you want to install inside the cages as well.

## Administration console errors and solutions

The following are some common administration console errors and solutions:

- [Login screen hangs](#)
- [SSH failed connection](#)
- [Missing Java or wrong Java version](#)
- [Time out](#)

### Login screen hangs

If the console login hangs or you experience other odd behavior, try to run the console from the command line to see any errors that come up.

To run the console from the command line

- 1 At the Windows command prompt type:

```
cd %cd%\Program Files\Symantec\Decoy Server\i
```

- 2 To run the console type:

```
java -jar mtadmin.jar
```

### SSH failed connection

In rare cases, when attempting to SSH into the host you may receive a “connection refused” error message. This means another user has connected to that particular port, and as such “stole” the SSH connection from the administrator. Because SSH requires authentication, a “stolen” port is typically benign. Restart SSH from the administration console and attempt to connect again.

### Missing Java or wrong Java version

Java 1.4 may not be installed on the machine or the wrong version of Java might be installed. In Solaris, check the version with the `java -version` command. In Windows, refer to the Java Readme.

## Time out

If a “Receive Time Out” error is reported when trying to connect to the host from the administration console, you may be experiencing one of the following problems:

- [Host is down](#)
- [Wrong IP address](#)
- [Wrong administrative interface set](#)
- [Incorrect user name or passphrase](#)
- [Stealthd is down](#)
- [Wrong port](#)
- [Network is down](#)

### Host is down

The host machine may have been shut down, or the cages could be loading. It takes approximately 10 minutes for a 4-cage system to load after a system restart. Make sure the host is fully loaded and attempt to connect to the host again.

### Wrong IP address

Make sure that the IP address in which you are connecting is the correct address of the host. The IP address is listed next to the host icon in the administration tree.

### Wrong administrative interface set

If you can not connect to the host from the administration console, make sure that the device value in the `<rtihome>/etc/qsp.conf` configuration file is set to the administrative interface, typically `hme0`. The administrative daemon will only bind and listen on this interface.

### Incorrect user name or passphrase

If the user name or passphrase is incorrect, you will not be able to connect to the host. Edit the host connection parameters to ensure that the user name and passphrase are accurate. If you are the first administrator, the user name is set to “admin” (unless it was edited on the host), and the passphrase is the passphrase you entered during the installation.

## Stealthd is down

The stealthd service may be down, therefore the host is not listening. Log on to the host and enter the following:

```
# ps -ef | grep stealthd
```

If stealthd is not running, restart the host machine.

## Wrong port

Verify that there is connectivity between the host and administration console machines. By default Symantec Decoy Server sets the stealth port number to 12387. However, if you changed the port number, be sure to reflect the changes by editing the host connection parameters.

## Network is down

The network may be experiencing problems. Check your connections, routers, and firewalls to make sure your network is functioning properly and attempt to reconnect.

# Alerting errors and solutions

The following are some common alerting errors and solutions:

- [Wrong SMTP gateway](#)
- [Wrong email address](#)
- [Wrong mail server](#)

## Wrong SMTP gateway

Ensure that there is a mailhost entry in /etc/hosts for the SMTP gateway you would like to use. Also ensure that you have the appropriate routes and connectivity to the SMTP gateway. Manually send a SMTP response to view the communication between Symantec Decoy Server and the mail host. See [“Initiating a response”](#) on page 72.

## Wrong email address

Ensure that you enter the correct email for the SMTP response. Also, verify that the host machine can reach the mail server. To do so, telnet from the host machine to the mail server over port 25. If you are unable to connect, there is

probably no mail connectivity between the machines and email alerting will not work.

## Wrong mail server

Do an nslookup of the mail exchanger to make sure Symantec Decoy Server is sending mail to the correct server.

```
# nslookup -type=mx <domain name>
```

Then send a manual SMTP response to view the communication between Symantec Decoy Server and the mail host. See [“Initiating a response”](#) on page 72.

## iButton errors and solutions

If Symantec Decoy Server reports an iButton error in the event logs, you may be experiencing one of the following problems:

- [iButton expired](#)
- [Wrong communication port](#)
- [Cable not securely attached](#)
- [iButton not securely seated](#)

### iButton expired

If the iButton expires, the host remains running but all cages automatically stop running. You must replace the iButton to start the cages. See [“Replacing a faulty or expired iButton”](#) on page 133.

Users can still log into the administration console after the iButton expires to view the log data and change configuration values on the host. However, if you restart the host after the iButton expires, the Symantec Decoy Server software will not reload.

---

**Warning:** Do not restart the host machine if the iButton has expired.

---

### Wrong communication port

Ensure that the proper iButton device is selected. The iButton device can be viewed and edited in the host General tab.

## Cable not securely attached

Ensure that the iButton caddy is properly attached to the appropriate communication port.

## iButton not securely seated

Ensure that the iButton is securely seated inside the caddy.

# Testing an iButton

The following instructions assume that Symantec Decoy Server is already installed. See [“Replacing a faulty or expired iButton”](#) on page 133.

To test the iButton

- 1 Assuming volume management is running, enter the volcheck -v command.
- 2 Change to the <rti\_home>/bin/util directory.
- 3 Execute the ibtest command, which requires the following usage:

```
# ./ibtest <ibdev> <dest>
```

where <ibdev> is the device in which the iButton is attached (typically /dev/ttyb) and <dest> is the iButton installation (typically <rti\_home>/etc). For example:

```
# ./ibtest /dev/ttyb /usr/decoy/etc
```

## Replacing a faulty or expired iButton

These instructions assume that Symantec Decoy Server is already installed.

To replace a faulty or expired iButton

- 1 Physically remove the old iButton from the DB9 serial port, and replace it with the new one.
- 2 Insert the new iButton diskette into the floppy drive.
- 3 Assuming volume management is running, enter the volcheck -v command.
- 4 Change to the <rti\_home>/bin/util directory.
- 5 Execute the ibinst command, which requires the following usage:

```
# ./ibinst <ibdev> <src> <dest>
```

where <ibdev> is the device in which the iButton is attached (typically /dev/ttyb), <src> is the source directory in which the iButton certificate is stored

(typically /floppy/floppy0), and <dest> is the destination directory in which the iButton certificate is installed (typically <rti\_home>/etc). For example:

```
# ./ibinst /dev/ttyb /floppy/floppy0 /usr/decoy/etc
```

- 6 Test the new iButton. See “[Testing an iButton](#)” on page 133.
- 7 Restart the machine.

## Cage failure

If the cage health icon indicates that the cage crashed, determine the cause of the failure and the processes that failed by viewing the cage logs. In the Description field of the log record, often the module will report the error that occurred. If you determine the cause of the crash, restart the machine and wait for the cage to load. If you are still having problems, visit <http://www.symantec.com/techsupp/>.

## Reporting problems

When reporting a problem, please have the following information available:

- Symantec Decoy Server version
- OS version

---

**Note:** When connected to a host you can get information on the host operating system, Symantec Decoy Server version number, and disk usage by clicking **Get Host Info...** in the **Host** menu.

---

- Copy of contents in the <rti\_home>/db directory
- Current system status-systems up and down, run checkconfig
- Details of debugging attempts-what has been done so far to triage the problem

## Event Types

This chapter includes the following topics:

- [Host events](#)
- [Cage events](#)

## About event types

Symantec Decoy Server uses modules to monitor the host and cages, and each module identifies itself to the logging daemon in order to report the location in which the data originated.

Defined are the modules, the columns each module reports, and the events associated therein.

## Host events

Host events include the following sections:

- [Administrative \(rti.admind\) events](#)
- [Stealth \(rti.stealthd\) events](#)
- [All module events](#)
- [Kernel \(rti.klogd\) events](#)
- [Proc \(rti.procf\) events](#)
- [Sysblock \(rti.sysblock\) events](#)
- [Filesystem \(rti.filesys\) events](#)

# Administrative (rti.admind) events

The following table describes rti.admind events:

Table A-11      Connection (rti.admind) events

Response policy event	Log viewer event, description and response	Priority
Admin Daemon Error	<p>adminind_error</p> <p><b>General:</b> Symantec Decoy Server's rti.admind experienced an error.</p> <p><b>Description:</b> The Symantec Decoy Server administration daemon sends this event whenever it encounters an error. The exact error message can be retrieved from the description field.</p> <p><b>Response:</b> Use the description field to direct further investigations.</p>	64

## Stealth (rti.stealthd) events

The following table describes rti.stealthd events:

Table A-12      Stealth (rti.stealthd) events

Response policy event	Log viewer event, description and response	Priority
User Logins	<p>stealthd_good_authentication</p> <p><b>General:</b> A Symantec Decoy Server Administration console successfully authenticated to the stealth service.</p> <p><b>Description:</b> A client successfully authenticated to the Symantec Decoy Server stealth service. This is the first step to establishing a connection to the administration daemon or to establishing a stealth SSH connection. The name of the user and the source IP address are recorded for audit purposes.</p>	64
Unsuccessful User Login	<p>stealthd_bad_authentication</p> <p><b>General:</b> A Symantec Decoy Server Administration console failed to authenticate.</p> <p><b>Description:</b> The stealthd received a correctly formatted request but the request failed to authenticate. Either the user does not exist in the password file (by default, /usr/decoy/etc/passwd) or the password was wrong. The actual error message is provided in the Description field of the log record.</p> <p><b>Response:</b> If the description reads "Failed login: No such user" then make sure the user appears in the &lt;rti_home&gt;/decoy/etc/passwd file.</p> <p>If the description reads "Failed login: Bad authentication" then ensure that the password used by the user is the same as the one supplied to the mtadduser command.</p> <p>If a stealthd_bad_authentication is followed immediately by a stealthd_good_authentication event then it is likely the user merely mis-typed the password.</p> <p>If a stealthd_bad_authentication is preceded or followed by a number of other stealthd error events then this might be part of an attempt to compromise the stealth service.</p>	64

Table A-12 Stealth (rti.stealthd) events

Response policy event	Log viewer event, description and response	Priority
Admin Server Start	<p>stealthd_server_start</p> <p><b>General:</b> Symantec Decoy Server's rti.stealthd started a service.</p> <p><b>Description:</b> An authenticated client has requested that the stealthd start the qsp proxy or sshd server. Though the stealthd can be configured to start almost any networked service, Symantec Decoy Server only uses two. The first, qsp proxy, is used to communicate with the administration daemon (rti.admind) and the logging database (logdb). The second is sshd, used to accept a single ssh client connection.</p> <p>This event is triggered every time a Symantec Decoy Server administration console connects to the Symantec Decoy Server host.</p> <p><b>Response:</b> Make sure that the program started (from the args field) is the same as the ones listed in the &lt;rti_home&gt;/decoy/etc/qsp.conf file. If not then this might be an attempt by an authorized user to circumvent security policy.</p> <p><b>Possible False Positive:</b> The stealthd records the command line of the service started. If the configuration has changed since a server was started then the commands may not match.</p>	32
Bad Packet	<p>stealthd_bad_packet</p> <p><b>General:</b> The Symantec Decoy Server stealthd has received an invalid packet.</p> <p><b>Description:</b> A packet that does not contain a valid stealth request has been received by the stealthd. This can either be a UDP port scan looking for services, or a mis-configured client expecting a different service on the same port.</p> <p>A client cannot distinguish between a bad authentication, a garbled packet and the stealth service not running. In any case, the client is sent an ICMP Port Unreachable message.</p> <p><b>Response:</b> Investigate the source of the bad packets. The IP address of the source machine is recorded in the ip-src field of the event.</p> <p><b>Possible False Positive:</b> It is possible, though very unlikely, that a device between a valid client and the stealthd service is corrupting the packets. The source machine may be incorrectly configured to use the stealthd port for some other service. In this case, consider fixing the misconfigured machine or changing the stealthd port in the &lt;RTIHOME&gt;/etc/qsp.conf configuration file.</p>	65

Table A-12 Stealth (rti.staltd) events

Response policy event	Log viewer event, description and response	Priority
Fatal Error	<p>staltd_fatal</p> <p><b>General:</b> The Symantec Decoy Server staltd failed to start up correctly and will exit.</p> <p><b>Description:</b> The staltd has encountered a catastrophic error and cannot continue. This event is triggered whenever the staltd encounters a problem from which it cannot continue. Examples include the allocation of memory, reading startup files, or initializing the network resources. A full description of the problem encountered is provided in the description.</p> <p><b>Response:</b> Investigate the error provided in the description field.</p>	128
User Logout	<p>staltd_server_stop</p> <p><b>General:</b> A Symantec Decoy Server administration service has finished.</p> <p><b>Description:</b> The qsp proxy or sshd service stopped. The process ID (PID) of the staltd_server_stop event should match the PID of a the staltd_server_start event.</p>	32
Admin Replay	<p>staltd_replay</p> <p><b>General:</b> An attempt to replay a successful authentication to a Symantec Decoy Server host has been thwarted.</p> <p><b>Description:</b> The stealth client uses a unique session identifier for each client connection. If the same session identifier is seen twice by the staltd, this could be an attempt to replay authentic traffic and gain unauthorized access. This event records the fact that a replay attempt was made and rejected.</p> <p><b>Response:</b> The client IP addresses is recorded in the event record. If the replay attempts continue then investigation of the machine owning that IP is in order.</p> <p><b>Possible False Positive:</b> It is possible, though highly unlikely, that this event could be triggered by a client with an extraordinarily bad random number generating routine.</p>	127

Table A-12 Stealth (rti.stealthd) events

Response policy event	Log viewer event, description and response	Priority
Error	<p>stealthd_error</p> <p><b>General:</b> The Symantec Decoy Server stealth service was not able to send a reply to a client.</p> <p><b>Description:</b> The stealthd encountered an error while trying to create and send a reply to a client. This is typically a symptom of a network configuration problem. The Description field of the event will include the full error description as provided by the strerror (3c) function.</p> <p><b>Response:</b> Use the description to further isolate the problem.</p>	64
Admin Server Fatal Error	<p>stealthd_server_fatal</p> <p><b>General:</b> A started Symantec Decoy Server administration process failed.</p> <p><b>Description:</b> A request to start the qsp proxy or sshd service from the stealthd failed. This can occur for reasons such as a missing executable, a bad &lt;rti_home&gt;/decoy/etc/qsp.conf file, or a problem with the service. See the description field of the event for more details.</p> <p><b>Response:</b> Use the description field to investigate the cause of the failure.</p>	127
Decoy Admin Timeout	<p>stealthd_server_timeout</p> <p><b>General:</b> A Symantec Decoy Server client failed to connect to service within timeout.</p> <p><b>Description:</b> In order to minimize the exposure of servers started by the stealthd, they are automatically stopped if the client does not connect to them within a configurable timeout. When the servers are stopped this event is sent.</p> <p>The most likely cause of this event is a Symantec Decoy Server administration console starting the sshd service on the Symantec Decoy Server host, and the user failing to connect their ssh client within the 60 second timeout period.</p> <p><b>Response:</b> If this event occurs often consider modifying the &lt;rti_home&gt;/decoy/etc/qsp.conf configuration to specify a larger timeout variable.</p>	1

# All module events

The following table describes all module events:

Table A-13 All module events

Response policy event	Log viewer event, description and response	Priority
Symantec Decoy Server Process Warning	warning  <b>General:</b> This is a Symantec Decoy Server operational warning.  <b>Description:</b> A module has encountered a recoverable problem. The warning is sent to indicate that non-normal behavior has occurred and there might be side effects.  <b>Response:</b> Investigate the situation using the module and description fields.	32
Symantec Decoy Server Process Error	error  <b>General:</b> This is a Symantec Decoy Server operational error.  <b>Description:</b> A module has encountered an unrecoverable error and may have ceased to function properly.  <b>Response:</b> Use the module and description fields to investigate the cause of the error.	128
None	info  <b>General:</b> This is Symantec Decoy Server operational information.  <b>Description:</b> This event is informational only and does not require any response.	8

# Kernel (rti.klogd) events

The following table describes rti.klogd events:

Table A-14      Kernel (rti.klogd) events

Response policy event	Log viewer event, description and response	Priority
Log Buffer Overrun	<p>buffer_overflow</p> <p><b>General:</b> Too many messages logged at once from the Symantec Decoy Server kernel logger.</p> <p><b>Description:</b> In order to optimize for speed and efficiency, Symantec Decoy Server uses a fixed size buffer to transfer messages from its kernel modules to the logging system. This event indicates that too many events were generated in a short amount of time.</p> <p><b>Response:</b> No response is necessary. The communications buffer will be emptied by the logger and normal operation will continue. However, the events leading up to the buffer_overflow should be investigated.</p>	239

## Proc (rti.procfs) events

The following table describes rti.procfs events:

Table A-15      Proc (rti.procfs) events

Response policy event	Log viewer event, description and response	Priority
Blocked Procfs Cage Escape	<p>blocked_procfs_cage_escape</p> <p><b>General:</b> Symantec Decoy Server blocked an intruder’s attempt to escape the cage through the /proc filesystem.</p> <p><b>Description:</b> The /proc file system provides a filesystem interface to the system processes; represented as directories containing informational files as well as links to the processes’ root directory and current working directory (cwd).</p> <p>Changing to the cwd or root directory of a /proc entry changes to the actual directory. This behavior can be exploited on some deception systems to escape the caged environment. Symantec Decoy Server records this event to indicate that such an attempt was made and thwarted.</p> <p><b>Response:</b> Look for indications of an established session or running trojan process that attempted the escape. The process id from this event can be used to find an associated exec or root_exec event. These events will record the actual command line used to execute the process.</p> <p>Also look for a corresponding stream_read event with the actual cd command if this was during an interactive session. If so the Symantec Decoy Server Administration console can be used to replay the entire session.</p>	128

## Sysblock (rti.sysblock) events

The following table describes the rti.sysblock events:

Table A-16 Sysblock (rti.sysblock) events

Response policy event	Log viewer event, description and response	Priority
Blocked Module Load/ Blocked Module Unload	blocked_modload/blocked_modunload <b>Description:</b> An attempt to load/unload a kernel module was blocked.	128
Blocked Mount/ Blocked Unmount	blocked_mount/blocked_umount <b>Description:</b> An attempt to mount/umount a filesystem was blocked.	128
Blocked Signal	blocked_signal <b>Description:</b> An attempt to send a signal to a process was blocked.	128

## Filesystem (rti.filesys) events

The following table describes the rti.filesys events:

Table A-17      Filesystem (rti.filesys) events

Response policy event	Log viewer event, description and response	Priority
Blocked DotDot Cage Escape	<p>blocked_dotdot_cage_escape</p> <p><b>General:</b> An attempt to escape a Symantec Decoy Server cage with ../ was blocked.</p> <p><b>Description:</b> An intruder entered a file path that included ../ , which could indicate an attempt to escape the chroot'ed cage environment. Symantec Decoy Server reports this event to indicate that the attempt was blocked and that the user or process is still in the cage.</p> <p><b>Response:</b> Look for indications of an established session or running trojan process that attempted the escape. The process id from this event can be used to find an associated exec or root_exec event. These events will record the actual command line used to execute the process.</p> <p>Also look for a corresponding stream_read event with the actual 'cd' command if this was during an interactive session. If so, the administration console can be used to replay the entire session.</p>	128

# Cage events

Cage events include the following sections:

- File (rti.strlog) events
- Process (rti.proclog) events
- File (rti.filelog) events
- Sniffer (rti.sniffd) events

## File (rti.strlog) events

The following table describes rti.srlog events:

Table A-18      File (rti.strlog) events

Response policy event	Log viewer event, description and response	Priority
Stream Open	<p>new_stream</p> <p><b>General:</b> A new PTY stream was created in a Symantec Decoy Server cage.</p> <p><b>Description:</b> A new pseudo terminal (pty7D) session has been created. This is the beginning of an interactive session and can be used to begin the replay of that session. The new_stream event signifies the beginning of an interactive session and can be used to begin the replay of that session.</p> <p><b>Response:</b> Look for subsequent stream_read and stream_write events and a final stream_close for a full audit of what happened on the pty. Also, the administration console can replay a session based on the stream data.</p>	128
Stream Close	<p>stream_close</p> <p><b>General:</b> A stream in a Symantec Decoy Server cage closed.</p> <p><b>Description:</b> This event indicates the end of a pty7D stream session.</p> <p><b>Response:</b> The administration console can replay a session based on the stream data.</p>	32

Table A-18 File (rti.strlog) events

Response policy event	Log viewer event, description and response	Priority
Stream Read Data	<p>read_stream_data</p> <p><b>General:</b> Data read from a stream in a Symantec Decoy Server cage.</p> <p><b>Description:</b> Keystrokes are being entered during an pty7D session with the cage. A corresponding stream_write will contain the terminal response, if any, to the input characters. In addition, there may be corresponding TCP_packet_ASCII_data if the pty was opened in response to a connection using a text protocol such as telnet.</p> <p>The interactive session may contain a variety of events, perhaps, mimicing an attacker logged into the cage attempting to further compromise the system.</p> <p><b>Response:</b> The Symantec Decoy Server Administrator's console can replay a session based on the stream data.</p>	96
Stream Write Data	<p>write_stream_data</p> <p><b>General:</b> Data was written to a stream in a Symantec Decoy Server cage.</p> <p><b>Description:</b> This represents the output written to the screen during an interactive pty7D session. A corresponding stream_read will contain the keystrokes the intruder entered, if any. In addition, there may be corresponding TCP_packet_ASCII_data if the pty was opened in response to a connection using a text protocol such as telnet.</p> <p>The interactive session may contain a variety of events, perhaps, mimicing an attacker logged into the cage attempting to further compromise the system.</p> <p><b>Response:</b> The Symantec Decoy Server Administrator's console can replay a session based on the stream data.</p>	48

## Process (rti.proclog) events

The following table describes rti.proclog events:

**Table A-19** Process (rti.proclog) events

Response policy event	Log viewer event, description and response	Priority
Normal User Execution	<p>exec</p> <p><b>General:</b> A process without root privileges was started within a Symantec Decoy Server cage.</p> <p><b>Description:</b> A user may have simply logged into the cage, or a successful exploit may have been launched that gives an attacker root capabilities. The Arguments column displays the name of the command that was executed; indicating whether the process is a shell, such as sh, ksh, bash, or csh, or a normal system maintenance process.</p> <p><b>Response:</b> Investigate the process parent (ppid) an indication of how this process started. If the parent normally does not spawn children then this could be a buffer overflow or other exploit.</p> <p>In addition, investigate associated events such as stream_read and stream_write, which can be used to replay the session, and file_open_writable which could indicate root privileges being used to alter system configuration.</p> <p><b>Possible False Positive:</b> A clever attacker may rename an executable to mask its real purpose. Also, normal system activity such as scheduled tasks (crond) can execute processes.</p>	96

Table A-19      Process (rti.proclg) events

Response policy event	Log viewer event, description and response	Priority
Root User Execution	<p>root_exec</p> <p><b>General:</b> A process with root privileges was started within a Symantec Decoy Server cage.</p> <p><b>Description:</b> This process could be the root user actually logging into the cage, or it could be a successful exploit giving a non-root user root capabilities. All processes started within the cage with root capabilities (uid=0, euid=0, gid=0, egid=0) will trigger this event.</p> <p><b>Response:</b> The arguments (args) field will indicate the name of the command that is executed. This is a good indication if this process is a shell (sh, ksh, bash, csh, etc) or a normal system maintenance process. However, it is possible that a clever attacker will rename an executable to mask its real purpose. Investigate the process parent (ppid) for indications of how this process started. If the parent normally does not spawn children then this could be a buffer overflow or other root exploit.</p> <p>In addition, investigate associated events such as stream_read and stream_write, which can be used to replay the session, and file_open_writable which could indicate root privileges being used to alter system configuration files.</p> <p><b>Possible False Positive:</b> Normal system activity such as scheduled tasks (crond) can execute processes with root capabilities. In addition, some network daemons will execute with root privileges and then drop them after initial configuration.</p>	128

## File (rti.filelog) events

The following table describes rti.filelog events:

Table A-20 File (rti.filelog) events

Response policy event	Log viewer event, description and response	Priority
Bad Device File Opened	<p>bad_device_file_opened</p> <p><b>General:</b> Symantec Decoy Server denied a request to open a device file (typically in /dev).</p> <p><b>Description:</b> Symantec Decoy Server blocks access to many system device files, such as the network devices that are not assigned to the cage. The user or process in the cage is given a “No such device” error and this event is triggered.</p> <p><b>Response:</b> The major and minor number of the device can be used to determine exactly which device access was blocked. The file /etc/name_to_major on the host (not in the cage) contains a mapping of name to major number for all devices. The minor number is an instance of the major device driver.</p> <p>In addition, stream_read and stream_write events or a TCP_packet_ASCII_data may contain more detailed data regarding what session was attempting to open the device.</p>	128
File Opened for Writing	<p>file_open_writable</p> <p><b>General:</b> A file has been opened for writing by a process in a Symantec Decoy Server cage.</p> <p><b>Description:</b> This event does not necessarily indicate that data is actually written to the file, though this is normally the case. You can use the process ID and user ID to determine why the file was opened. Many system processes open system account files for writing. A prime example of this is /var/adm/utmpx which is opened repeatedly in normal system operation.</p> <p><b>Response:</b> Determine if this file is normally written by the recorded process. A related exec or root_exec event will record the actual process name and arguments associated with the process id. Stream_read and stream_write events can be used to replay the corresponding session for more information on what may have been written to the file.</p> <p><b>Possible False Positive:</b> Many system processes open system account files for writing. A prime example of this is /var/adm/utmpx which is opened repeatedly in normal system operation.</p>	64

## Sniffer (rti.sniffd) events

The following table describes rti.sniffd events:

Table A-21 Sniffer (rti.sniffd) events

Response policy event	Log viewer event, description and response	Priority
Outgoing TCP Connection	<p>outgoing_connection</p> <p><b>General:</b> An outgoing TCP connection attempt from a Symantec Decoy Server cage was detected.</p> <p><b>Description:</b> A TCP connection from the IP address (ip-src) is being established to another IP address (ip-dest). This is typically a connection from a cage to another host. If the cage's network interface card has been placed in promiscuous mode, this could indicate a connection being established from the local LAN segment.</p> <p>The source IP should match that of a Symantec Decoy Server cage. The destination port can be used to determine the service to which the attacker is attempting to connect. This event is triggered when the cage interface receives a packet with the TCP SYN and ACK flags set. The packet is sent as the second part of the TCP three-way handshake and means that another host is acknowledging a connection request from the cage.</p> <p><b>Response:</b> If the connection is from the Symantec Decoy Server cage then there will be other logged events both before and after this one. Look for related events within the same time period to determine how the attacker gained access to the cage and what program they are attempting to connect with.</p> <p>TCP_packet_ASCII_data events with the same source and destination IPs and ports may reveal more information on the contents of the TCP connection. For example if the connection is to an FTP server then the destination port will likely be port 21 and the entire transcript of the session will be reported through TCP_packet_ASCII_data events.</p> <p>The destination port can be used to help determine the likely program or protocol being used on the connection, /etc/services lists common ports and corresponding services. A large number of outgoing_connection events with either increasing or decreasing port numbers may indicate that a port scan using a tool such as nmap is being initiated from within the cage.</p> <p><b>Possible False Positives:</b> If the NIC is in promiscuous mode, the source IP will not match that of a cage. If a service on the host is configured to bind to all interfaces, then incoming connections to the cage interface may be received by a host service. This configuration should be avoided.</p>	128

Table A-21 Sniffer (rti.sniffd) events

Response policy event	Log viewer event, description and response	Priority
Inbound TCP Connection	<p>incoming_connection</p> <p><b>General:</b> An attempt, to establish an incoming TCP connection with Symantec Decoy Server, was made.</p> <p><b>Description:</b> This event is triggered before the TCP handshake is complete and therefore may not represent an entire connection. If the NIC is in promiscuous mode the destination IP will not match that of a cage. If the host has free access to all the cage interfaces it may, due to internal routing rules, make outgoing connections using the cage interfaces.</p> <p><b>Response:</b> Look for a large number of incoming_connection events with either increasing or decreasing port numbers. This likely represents a port-scan of the Symantec Decoy Server cage.</p> <p>A new_stream, root_exec, and/or exec event immediately following an incoming_connection indicates that a process inside the cage is accepting the incoming connection.</p> <p>The destination port can be used to help determine the likely program or protocol being used on the connection, /etc/services lists common ports and corresponding services. In addition, /etc/inetd.conf from the cage lists the programs automatically started by inetd (1M) in response to incoming connections on certain ports.</p> <p><b>Possible False Positives:</b> If the NIC is in promiscuous mode the destination IP will not match that of a cage. The host has free access to all the cage interfaces and may, due to internal routing rules, make outgoing connections using the cage interfaces.</p>	64

Table A-21      Sniffer (rti.sniffd) events

Response policy event	Log viewer event, description and response	Priority
ASCII Data in TCP Traffic	<p>TCP_packet_ASCII_data</p> <p><b>General:</b> Plain text data was found in a TCP packet going to or from a Symantec Decoy Server cage.</p> <p><b>Description:</b> This is the expected behavior of text-based protocols such as HTTP, FTP, and telnet. If this event is triggered with source and destination ports that do not match any text-based service (or that are used by a non-text-based service), this could indicate the use of a trojan back door program or a successful buffer overflow attack. It is also possible that the host may send data out of a cage interface.</p> <p><b>Response:</b> The presence of a related incoming or outgoing connection event will indicate whether this data is part of an inbound or outbound session. stream_read and/or stream_write events will likely mirror this event and can be used to replay the session.</p> <p>The presence of a root_exec, exec, and incoming_connection event in combination with a destination port for an otherwise binary service may indicate a successful buffer overflow attack.</p> <p><b>Possible False Positive:</b> The host has free access to all cage interfaces and may, due to internal routing rules, make outgoing connections using cage interfaces.</p>	32

**Table A-21** Sniffer (rti.sniffd) events

Response policy event	Log viewer event, description and response	Priority
Outgoing UDP Packet	<p>outgoing_udp_packet</p> <p><b>General:</b> An outbound UDP packet has been detected from a Symantec Decoy Server cage.</p> <p><b>Description:</b> The sniffer has detected a UDP packet with a source address matching the cage interface. Common uses of UDP include host name lookups (DNS) on port 53, logging information (syslog) on port 514, and rpc services on many ports such as 111.</p> <p>Some older denial of service (DoS) attacks would use UDP packets with a source port of echo (port 7) and a destination port of chargen (port 19) in an attempt to convince two or more machines to send UDP packets back and forth endlessly. If the NIC is in promiscuous mode the destination IP will not match that of a cage. It is also possible that the host may send data out of a cage interface.</p> <p><b>Response:</b> Look for related exec or root_exec messages for processes that could be sending the UDP packets. Often the source and destination ports can be used to help find what protocol and thus what program is sending the packets, /etc/services lists common ports and corresponding services.</p> <p><b>Possible False Positives:</b> If the NIC is in promiscuous mode the destination IP will not match that of a cage. Also, the host has free access to all cage interfaces and may, due to internal routing rules, send data using cage interfaces.</p>	128

Table A-21 Sniffer (rti.sniffd) events

Response policy event	Log viewer event, description and response	Priority
Incoming UDP Packet	<p>incoming_udp_packet</p> <p><b>General:</b> An inbound UDP packet has been detected in a Symantec Decoy Server cage.</p> <p><b>Description:</b> The cage has received a UDP packet with an IP address that matches that of the cage interface. Many services use UDP to communicate. The destination port of the packet can be used to help determine the target service. Common services include bind/DNS (53), syslog (514) and rpc portmap (111). If the NIC is in promiscuous mode the destination IP will not match that of a cage.</p> <p><b>Response:</b> The destination port can be used to help determine the likely program or protocol being targeted. /etc/services a list of common ports and the corresponding services. In addition /etc/inetd.conf from the cage lists the programs automatically started by inetd(1M) in response to incoming connections on certain ports.</p> <p>An outgoing_udp_packet with a destination matching the source of the incoming_udp_packet is likely a response to this packet. A root_exec or exec of a process with a parent process id matching a known UDP based server could indicate a buffer overflow attack.</p> <p><b>Possible False Positives:</b> If the NIC is in promiscuous mode the destination IP will not match that of a cage.</p>	64
UDP Packet Detected	<p>udp_packet_detected</p> <p><b>General:</b> A UDP packet has been detected in a Symantec Decoy Server cage.</p> <p><b>Description:</b> A UDP packet has been detected and the cage interface's IP address does not match either the source or the destination IP address of the UDP packet.</p> <p><b>Response:</b> See responses for <a href="#">incoming_udp_packet</a> and <a href="#">outgoing_udp_packet</a>. In addition, if the source and destination addresses do not match the cage or host interface, then, this is likely an attempt to forge a UDP packet.</p> <p><b>Possible False Positives:</b> If the NIC is in promiscuous mode the destination IP will not match that of a cage. Also, the host has free access to all cage interfaces and may, due to internal routing rules, send data using cage interfaces.</p>	64
ICMP Packet Detected	<p>icmp_packet_detected</p> <p><b>Description:</b> An ICMP packet was detected.</p>	64
Incoming ICMP Packet	<p>incoming_icmp_packet</p> <p><b>Description:</b> An incoming ICMP packet was detected.</p>	64

Table A-21       Sniffer (rti.sniffd) events

Response policy event	Log viewer event, description and response	Priority
Invalid ICMP packet	invalid_icmp_packet <b>Description:</b> An invalid ICMP packet was detected	64
Outgoing ICMP Packet	outgoing_icmp_packet <b>Description:</b> An outgoing ICMP packet was detected.	128



# Index

## A

### Account privileges

- user 51

### Administration console

- adding host connections 42
- adding local accounts 42
- adding user accounts 50
- cage status icons 46
- changing host passphrase 47
- connect to hosts 44
- disconnecting from hosts 47
- host status icons 45
- installing on Solaris 40
- installing on Windows 39
- starting and stopping 41
- system requirements 38
- troubleshooting 129
- uninstalling 41, 52
- viewing cages 45

### Alerts

- troubleshooting 131

### Attacks

- determining IP ownership 122
- taking legal action 123

## C

### Cage

- adding user accounts 90
- configuration 25
- content generation module (CGM) 4
- content tab 61
- creating custom cages 97
- database server protection 99
- events 147
- FTP server protection 99
- general description 2
- general tab 61
- legal disclaimer banner 100
- report data 77

- setting the cage root password 91

- setting the user password 90

- status icons 46

- viewing 45

- web server protection 98

### Cage events

- file activity module events 147, 151

- process module events 149

- sniffer module events 152

### Cage filter options

- filesystem module 70

- process module 70

- sniffer module 70

- streams module 70

### Cage processes

- rti.klogd 36

- rti.logd 36

- rti.maild 36

- rti.sniffd 36

- startcage 35

### Cage sessions

- editing CGM user accounts 92

- editing IP addresses 92

- establishing 92

- modifying bypassing log 95

- restoring cages 97

- starting and stopping 95

- updating backup files 96

### Configuration values

- configuring cages 30

- configuring hosts 30

### Content generation tools

- rti.deluser 36

- rti.listuser 36

- rti.makeuser 36

- rti.newusers 36

- rti.usergen 36

### Content tab

- cage 61

**D**

- Data display options
  - scheduling parameters 86
- Data filtering options
  - file filter 84
  - IP address filter 84
  - number of results to display 85
  - priority filter 83
  - user filter 85
- Deployment
  - getting started 8
- Deployment schemes
  - custom 11
  - Honey Net 10
  - Minefield 9
  - Shield 11

**E**

- Event types
  - cage events 147
  - host events 136

**G**

- General tab
  - cage 61
  - host 58

**H**

- Host
  - adding connections 42
  - changing passphrase 47
  - connect using SSH 48
  - connecting to 44
  - connection parameters 49
  - disconnecting from 47
  - editing connections using SSH 49
  - events 136
  - general tab 58
  - log tab 59
  - report data 77
  - status icons 45
- Host events
  - all module events 142
  - filesystem module events 146
  - kernel module events 143

- proc module events 144

- Host filter options
  - administrative management module 70
  - iButton module 70
  - Symantec Decoy Server processes module 70
- Host parameters
  - editing 58
- Host processes
  - cagemand 35
  - logdb 35
  - rti.admind 35
  - rti.confd 35
  - rti.ibuttond 35
  - rti.logd 35
  - rti.stealthd 35
- Host software
  - configuration 23
  - starting and stopping 33
  - upgrades 34

**I**

- iButton
  - general description 5
  - testing 133
  - troubleshooting 132
- Install
  - auto-install 31
  - configuring cages 25
  - configuring hosts 23
  - getting started 14
  - host system requirements 15
  - installing remote host 32
  - installing Solaris administration console 40
  - installing Solaris host 17
  - installing Windows administration console 39
  - loading a configuration 31
  - MAC addresses 19
  - mount points configuration 29
  - network interface cards 18
  - pre-installing host software 16
  - troubleshooting 126
  - uninstalling Symantec Decoy Server host 33
  - upgrading host software 34
  - verifying Solaris host installation 18

**L**

## Local accounts

- adding 42

## Log queries

- adding predefined queries 102
- cage log data 103
- custom queries 103
- editing custom queries 106
- host log data 102
- operators 105
- search parameters 104
- search values 104

## Log records

- automatically compressing 117
- column results 111
- compressing 117
- event priority 111
- exporting results 112
- printing results 112
- querying 107
- restoring backup logs 118
- restoring compressed logs 119
- rotating and compressing 115
- search limit 108
- search results 109
- sorting results 111
- trimming 116
- verification failure 114
- verify 113

## Log sessions

- PTY session replay 113
- replaying cage sessions 112

## Log tab

- host 59

**M**

## MAC addresses

- installation 19

**N**

## Network interface cards

- installation 18

**P**

## Parameters

- cage.conf 64

- command line 63

- host connection 49

- reports 76

- reverting changes 62

- rti.conf 63

- saving changes 62

**R**

## Report parameters

- data breakdown options 80

- data display options 85

- date range options 82

## Report policies

- adding 86

## Reports

- cage report data 77

- data display options 85

- data filtering options 83

- display options 87

- displaying results 85

- file filter options 84

- generating 86

- generating via log viewer 87

- host report data 77

- IP address filter 84

- results sort order 81

- scheduling parameters 86

- setting parameters 76

- troubleshooting 134

- user filter 85

## Response filters

- adding 71

- cage options 70

- description 69

- editing 72

- excluding 70

- format 69

- host options 70

- including 69

## Response policies

- adding 66

- characteristics 68

- modifying 68

- selecting events 68

- testing 72

## S

### Solaris

- host installation 17

- host installation verification 18

### SSH

- editing host connections 49

- to host 48

### Symantec Decoy Server

- definition of 2

- role in detection 3

- role in prevention 3

- role in response 3

## U

### User accounts

- privileges 51